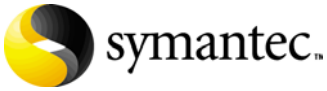
Symantec™ Gateway Security 400 Series

Administrator's Guide

Supported models:

Models 420, 440, 460, and 460R



Symantec™ Gateway Security 400 Series Administrator's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 2.1
June 23, 2004

Copyright notice

Copyright © 1998–2004 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. LiveUpdate, LiveUpdate Administration Utility, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

See “Licensing” on page 111.

Contacting Technical Support

Customers with a current maintenance agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp.

Customers with Gold or Platinum support agreements may contact Platinum Technical Support by the Gold or Platinum Web site at https://www-secure.symantec.com/gold or https://www-secure.symantec.com/platinum. When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
- Error messages/log files
- Troubleshooting performed prior to contacting Symantec
- Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com/techsupp, select the appropriate Global Site for your country, then select the enterprise Continue link. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec’s technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Chapter 1 Introducing the Symantec Gateway Security 400 Series

About Symantec Gateway Security 400 Series 11
Key features 11
- Firewall technology 12
- Virtual Private Network (VPN) technology 12
- Antivirus policy enforcement (AVpe) 12
- Static content filtering 12
- Intrusion detection and intrusion prevention (IDS and IPS) 12
- LiveUpdate support 12
- Managing Symantec Gateway Security 400 Series locally 12
- Managing Symantec Gateway Security 400 Series through SESA 13

Intended audience 14
Where to find more information 14
Network security best practices 15

Chapter 2 Administering the security gateway

Logging on to the Security Gateway Management Interface 17
Navigating the user interface 18
- Understanding left pane main menu options 19
- Understanding right pane features 19
- Tips for using the SGMI 20

Managing administrative access 20
- Setting the administration password 20
- Configuring remote management 21

Managing the security gateway using the serial console 23

Chapter 3 Configuring a connection to the outside network

About connecting to the outside network 25
Network examples 26
Understanding the Setup Wizard 29
About dual-WAN port appliances 30
Understanding connection types 31
Configuring connectivity 32
- DHCP 32
- PPPoE 32
- Static IP and DNS 35
- PPTP 36
- Dial-up accounts 37

Configuring advanced connection settings 40
- Advanced DHCP settings 40
- Advanced PPP settings 41
- Maximum Transmission Unit (MTU) 41

Configuring dynamic DNS 42
- Forcing dynamic DNS updates 43
- Disabling dynamic DNS 43

Configuring routing 44
- Enabling dynamic routing 44

Configuring static route entries 44
Configuring advanced WAN/ISP settings 45
High availability 45
Load balancing 46
SMTP binding 46
Binding to other protocols 47
Configuring failover 47
DNS gateway 47
Optional network settings 48

Chapter 4 Configuring internal connections

Configuring LAN IP settings 51
Configuring the appliance as a DHCP server 52
Monitoring DHCP usage 53
Configuring port assignments 53
Standard port assignment 53
SGS Access Point Secured port assignment 53
Enforce VPN tunnels port assignment 53

Chapter 5 Network traffic control

Planning network access 55
Understanding computers and computer groups 55
Defining computer group membership 56
Defining computer groups 57
Defining inbound access 58
Defining outbound access 59
Outbound rule example 60
Configuring services 61
Redirecting services 61
Configuring special applications 62
Configuring advanced options 64
Enabling the IDENT port 64
Disabling NAT mode 64
Blocking ICMP requests 65
Enabling WAN broadcast storm protection 65
Enabling IPsec pass-thru 65
Configuring an exposed host 66

Chapter 6 Establishing secure VPN connections

How to use this chapter 67
Creating security policies 68
Understanding VPN policies 68
Creating custom Phase 2 VPN policies 69
Viewing VPN Policies List 70
Identifying users 70
Understanding user types 70
Defining users 71
Viewing the User List 72
Configuring gateway-to-gateway tunnels 72
Understanding gateway-to-gateway tunnels 72
Configuring dynamic gateway-to-gateway tunnels 74
Configuring static gateway-to-gateway tunnels 75
Sharing information with the remote gateway administrator 77
Configuring client-to-gateway VPN tunnels 78

Understanding Client-to-Gateway VPN tunnels 78
Defining client VPN tunnels 80
Configuring global policy settings for client-to-gateway VPN tunnels 81
Sharing information with your clients 81
Monitoring VPN tunnel status 82

Chapter 7 Advanced network traffic control

How antivirus policy enforcement (AVpe) works 83
Before you configure AVpe 84
Configuring AVpe 85
Enabling AVpe 86
Configuring the antivirus clients 87
Monitoring antivirus status 87
Viewing AVpe log messages 87
Verifying AVpe operation 87
About content filtering 88
Managing content filtering lists 89
Enabling content filtering 89
Monitoring content filtering 90

Chapter 8 Preventing attacks

Intrusion detection and intrusion prevention 91
Atomic packet inspection 91
Trojan horse notification 92
Setting protection preferences 92
Enabling advanced protection settings 93
IP spoofing protection 93
TCP flag validation 93

Chapter 9 Logging, monitoring and updates

Managing logging 95
Configuring log preferences 95
Managing log messages 98
Updating firmware 99
Automatically updating firmware 99
Upgrading firmware manually 102
Checking firmware update status 104
Backing up and restoring configurations 105
Resetting the appliance 106
Interpreting LEDs 107
LiveUpdate and firmware upgrade LED sequences 108

Appendix A Troubleshooting

About troubleshooting 109
Accessing troubleshooting information 110

Appendix B Licensing

Appendix C Field descriptions

Logging/Monitoring field descriptions 119
Status tab field descriptions 120
View Log tab field descriptions 121
Log Settings tab field descriptions 122

Troubleshooting tab field descriptions ... 123
Administration field descriptions ... 123
Basic Management tab field descriptions ... 123
Advanced Management tab field descriptions ... 124
SNMP tab field descriptions ... 125
Trusted Certificates tab field descriptions ... 125
LiveUpdate tab field descriptions ... 126
LAN field descriptions ... 127
LAN IP & DHCP tab field descriptions ... 127
Port Assignments tab field descriptions ... 129
WAN/ISP field descriptions ... 129
Main Setup tab field descriptions ... 130
Static IP & DNS tab field descriptions ... 131
PPPoE tab field descriptions ... 131
Dial-up Backup & Analog/ISDN tab field descriptions ... 132
PPTP tab field descriptions ... 134
Dynamic DNS tab field descriptions ... 135
Routing tab field descriptions ... 136
Advanced tab field descriptions ... 138
Firewall field descriptions ... 139
Computers tab field descriptions ... 139
Computer Groups tab field descriptions ... 140
Inbound Rules field descriptions ... 141
Outbound Rules tab field descriptions ... 142
Services tab field descriptions ... 142
Special Applications tab field descriptions ... 143
Advanced tab field descriptions ... 145
VPN field descriptions ... 146
Dynamic Tunnels tab field descriptions ... 147
Static Tunnels tab field descriptions ... 150
Client Tunnels tab field descriptions ... 151
Client Users tab field descriptions ... 152
VPN Policies tab field descriptions ... 153
VPN Status tab field descriptions ... 154
Advanced tab field descriptions ... 155
IDS/IPS field descriptions ... 156
IDS Protection tab field descriptions ... 156
Advanced tab field descriptions ... 157
Antivirus Policy field descriptions ... 158
Content Filtering field descriptions ... 159

Appendix D Joining security gateways to SESA

About joining SESA ... 161
Preparing to join SESA ... 162
Trusted certificates ... 162
Joining Symantec Gateway Security 400 Series to SESA ... 163
Determining your options for joining SESA ... 163
Joining SESA ... 164
Viewing SESA Agent status ... 165
Understanding how security gateways obtain configurations from SESA ... 166
Logging on to the Symantec Management Console ... 166
Troubleshooting problems when joining SESA ... 166
Leaving SESA ... 166

Glossary

Chapter 1

Introducing the Symantec Gateway Security 400 Series

This chapter includes the following topics:

- About Symantec Gateway Security 400 Series
- Key features
- Intended audience
- Where to find more information
- Network security best practices

About Symantec Gateway Security 400 Series

The Symantec Gateway Security 400 Series appliances are Symantec's integrated security solution for enterprise remote and small branch office environments, with support for secure wireless LANs.

The Symantec Gateway Security 400 Series provides integrated security by offering six security functions in the base product:

- Firewall
- IPSec virtual private network (VPN) tunnels with hardware-assisted 3DES and AES encryption
- Antivirus policy enforcement (AVpe)
- Static content filtering
- Intrusion detection and intrusion prevention
- LiveUpdate support

Key features

All features are designed specifically for the small office environment. These appliances are perfect for stand-alone environments or as a complement to Symantec Gateway Security 5400 Series appliances deployed at hub sites.

All of the Symantec Gateway Security 300/400 Series models are wireless-capable. They have special wireless firmware and a CardBus slot that accommodates an optional wireless feature add-on, that consists of an integrated 802.11b/g radio card and antenna. When used with the appliance's VPN feature, the security gateway offers the highest possible integrated security for wireless LANs.

LiveUpdate of firmware strengthens the Symantec Gateway Security 400 Series security response, making it an ideal solution for remote or small branch offices.

Firewall technology

The Symantec Gateway Security 400 Series appliance protects enterprise assets and business transactions with one of the most secure, high-performance solutions for ensuring safe connections with the Internet and between networks. Its unique architecture delivers security and speed, providing strong and transparent firewall protection against unwanted intrusion without slowing the flow of approved traffic on enterprise networks.

Virtual Private Network (VPN) technology

Symantec Gateway Security 400 Series lets organizations securely extend their network perimeters beyond the security gateway by providing VPN server proxy-secured scanning and personal firewall protection using Symantec Client VPN. A completely integrated and standards-based solution, it lets organizations establish safe, fast, and inexpensive connections, enabling new forms of business and secure access to information for authorized partners, customers, telecommuters, and remote offices.

The security gateway appliance uses VPN tunnels to send encrypted and encapsulated IP packets over public networks securely to another VPN server.

Antivirus policy enforcement (AVpe)

Symantec Gateway Security 400 Series provides antivirus policy enforcement (AVpe) at the security gateway. Symantec Gateway Security 400 Series acts as an intermediary between Symantec AntiVirus Corporate Edition servers and clients. The appliance validates that the clients are up-to-date with their virus definitions prior to allowing inbound/outbound VPN client connections and other outbound traffic.

Static content filtering

Symantec Gateway Security 400 Series supports content filtering for outbound traffic using allow and deny lists controlled by groups of security gateway users. When a group is configured to use an allow list, the content filtering component filters and drops connection requests sent to a destination that does not match an entry in the allow list.

Likewise, when a group is configured to use a deny list, the content filtering component filters and drops connection requests sent to a destination that matches an entry in the deny list.

Intrusion detection and intrusion prevention (IDS and IPS)

Symantec Gateway Security 400 Series provides an intrusion detection and intrusion prevention component that protects internal network resources from attack by pinpointing malicious activities and identifying intrusions in real-time, letting you respond rapidly to the attacks.

LiveUpdate support

Symantec Gateway Security 400 Series incorporates patented LiveUpdate technology to keep your product up-to-date by downloading firmware updates.

Managing Symantec Gateway Security 400 Series locally

You can manage the full set of features of the Symantec Gateway Security 400 Series using the local interface, the Security Gateway Management Interface (SGMI). You can access the SGMI from an external Web browser by entering the appliance's WAN port IP address, and then supplying the administrator's user name and password.

The guide you are reading describes in detail the use of the SGMI.

See "Administering the security gateway" on page 15.

Managing Symantec Gateway Security 400 Series through SESA

Symantec Event Manager and Advanced Manager for Security Gateways (Group 2) v2.1 are integrated with the Symantec Enterprise Security Architecture (SESA) to provide a common framework to manage multiple Symantec Gateway Security 400 Series appliances and third-party products from a single, centralized location.

The SESA framework consists of a set of scalable, extensible, and secure technologies that make integrated security products interoperable and manageable, regardless of the size and complexity of your network.

When managing security gateways through SESA, you can manage multiple security gateways from a single user interface, regardless of the network on which your SESA Manager resides. You can group them to reflect your organizational structure and create common configurations that are shared by security gateways that have the same security postures.

The event management capabilities of Symantec Event Manager, installed with Symantec Advanced Manager, give you up-to-date information that you need to make informed decisions about the security of your network and related devices.

See the *Symantec Event Manager and Advanced Manager for Security Gateways (Group 2) v2.1 Administrator's Guide* for details on using the Symantec Management Console.

Symantec Advanced Manager for Security Gateways (Group 2) v2.1

Symantec Advanced Manager for Security Gateways is a software security solution, installed on the SESA Manager computer, that plugs into the Symantec management console. It provides a Web-based graphical user interface through which you can monitor and organize a large number of security gateways, along with other SESA-compliant products.

Advanced management through SESA lets you manage both policies and location settings of connected security gateways, in addition to collecting events from those systems. SESA management also provides scalable management by allowing multiple security gateways to share common policies and location settings.

SESA management provides many features important to centralized and scalable management, including:

- Logical grouping of security gateways into organizational units
- Management of multiple configurations
- Sharing of configurations across security gateways
- Validation of multiple configurations in a single action
- Distribution of configurations to many security gateways in a single action

The Symantec Advanced Manager also includes the Symantec Event Manager for Security Gateways (Group 2) v2.1 product (described in the next section) for centralized event logging, alerting and reporting.

Symantec Event Manager for Security Gateways (Group 2) v2.1

Symantec Event Manager for Security Gateways is a standards-based software security solution that provides centralized logging, alerting, and reporting across Symantec's security gateway protection solutions and select third-party products.

Symantec Event Manager delivers security information to the SESA DataStore, letting you see a centralized, consistent view of your security events from the Symantec management console. Security events and log messages can be viewed in a variety of predefined or custom report formats.

By collecting and formatting information from Symantec and third-party supported products, the Symantec Event Manager consolidates and normalizes security event data, making impending threats more easily identifiable.

Combining powerful alert notification, enterprise reporting and role-based administration with a highly scalable secure architecture, the Symantec Event Manager is ideally suited for medium-to-large enterprises and supported security services environments.

If you have separately purchased an Event Collector for a third-party firewall product, you can also view events generated by that product.

Symantec Event Manager for Security Gateways is installed on the SESA Manager computer. You join each local security gateway to SESA using the controls provided in the Security Gateway Management Interface (SGMI).

Symantec Event Manager is automatically installed if you install the Symantec Advanced Manager for Security Gateways.

Intended audience

This manual is intended for system managers or administrators responsible for installing and maintaining the security gateway. It assumes that readers have a solid base in networking concepts and an Internet browser.

Where to find more information

The Symantec Gateway Security 400 Series functionality is described in the following manuals:

- *Symantec™ Gateway Security 400 Series Administrator's Guide*
  The guide you are reading describes how to configure the firewall, VPN, AntiVirus policy enforcement (AVpe), content filtering, IDS, IPS, LiveUpdate, and all other features of the security gateway appliance. It is provided in PDF format on the Symantec Gateway Security 400 Series software CD-ROM.
- *Symantec™ Gateway Security 400 Series Installation Guide*
  This guide describes in detail how to install the security gateway appliance and run the Setup Wizard to get connectivity.
- *Symantec™ Gateway Security 400 Series Quick Start Card*
  This card provides abbreviated instructions for installing your appliance.
- *Symantec™ Gateway Security 400 Series Getting Started Guide*
  This guide lists the tasks that you need to perform after installing the appliance.
- *Symantec™ Gateway Security 400 Series Release Notes*
  This document provides a summary of new and changed product features, system requirements, and issues and workarounds.
- *Symantec™ Gateway Security 300/400 Series Wireless Implementation Guide*
  This guide describes how to install and configure the wireless LAN card in the appliance to create a secure WLAN.
- *Symantec™ Gateway Security 300/400 Series Wireless Release Notes*
  This document provides a summary of new and changed product features, system requirements, and issues and workarounds.
- *Symantec™ Event Manager and Advanced Manager for Security Gateways (Group 2) v2.1 Integration Guide*
  This guide describes how to integrate the Symantec security gateway into the SESA environment.
- *Symantec™ Event Manager and Advanced Manager for Security Gateways (Group 2) v2.1 Administrator's Guide*
  This guide describes how to administer Symantec security gateways from the SESA environment using the Symantec Advanced Manager and Symantec Event Manager products.

- *Symantec™ Event Manager and Advanced Manager for Security Gateways (Group 2) v2.1 Release Notes.* This document provides a summary of new and changed product features, system requirements, and issues and workarounds.

Network security best practices

Symantec encourages all users and administrators to adhere to the following security practices:

- Turn off and remove unneeded services.
  By default, many operating systems install auxiliary services that are not critical, such as an FTP server, Telnet, and a Web server. These services are avenues of attack. If they are removed, blended threats have less avenues of attack and you have fewer services to maintain through patch updates.
- If a blended threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
- Turn off unnecessary network services.
- Automatically update your antivirus at the gateway, server, and client.
- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the security gateway, such as HTTP, FTP, mail, and DNS services.
- Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files.
- Hackers commonly break into a Web site through known security holes, so make sure your servers and applications are patched and up to date.
- Eliminate all unneeded programs.
- Isolate infected computers quickly to prevent further compromising your organization. Perform a forensic analysis and restore the computers using trusted media.
- Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

Additional information, in-depth white papers, and resources regarding enterprise security solutions can be found by visiting the Symantec Enterprise Solutions Web site at http://enterprisesecurity.symantec.com.

Chapter 2

Administering the security gateway

This chapter includes the following topics:

- Logging on to the Security Gateway Management Interface
- Navigating the user interface
- Managing administrative access
- Managing the security gateway using the serial console

Logging on to the Security Gateway Management Interface

Symantec Gateway Security 400 Series appliances are managed using a browser-based console called the Security Gateway Management Interface (SGMI). The SGMI is a standalone management console for local management and log viewing.

Use one of the following supported Web browsers to connect to SGMI:

- Microsoft Internet Explorer version 5.5 or 6.0 SP1
- Netscape version 6.23 or 7.0

To ensure compatibility with Web site using older HTTP, you may need to clear the proxy settings in the browser before connecting to the SGMI.

Install the appliance according to the instructions in the *Symantec Gateway Security 400 Series Quick Start Card* or the *Symantec Gateway Security 400 Series Installation Guide* before connecting to the SGMI.

The interface you see when you connect to the SGMI may vary slightly depending on the model you are managing because the number of LAN and WAN ports differs between models as shown in Table 2-1.

Table 2-1 Interfaces by model

Model	Number of WAN ports	Number of LAN ports	Number of serial (modem) ports
420/440	1	4	1
460/460R	2	8	1

To connect to the SGMI

You can connect to the SGMI either locally or remotely.

To connect to the SGMI locally

1. Browse to the LAN IP address of the appliance.
   The default appliance LAN IP address is 192.168.0.1.
2. On your keyboard, press **Enter**.
   The SGMI window displays (see Figure 2-1).

To connect to the SGMI remotely

1. Browse to the appliance's WAN port IP address followed by port 8088, for example: http://206.7.7.14:8088
2. On your keyboard, press **Enter**.
   The SGMI window displays (see Figure 2-1). If this is the first time you have connected, the Setup Wizard runs automatically.

Navigating the user interface

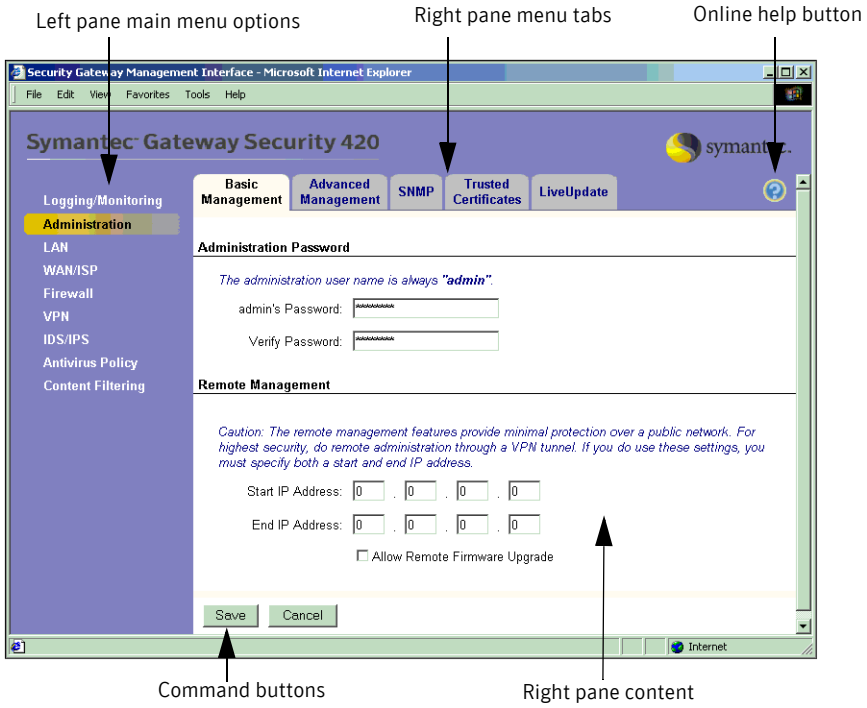
Once you familiarize yourself with the basic structure of the user interface, you can create configurations, view security gateway status, and access system event logs. The SGMI, shown in Figure 2-1, includes the following controls:

- Left pane main menu options
- Right pane menu tabs
- Right pane content
- Command buttons (bottom)
- Online Help button

Online help is available for each tab when you click the blue circle with a question mark in the top right corner of each screen.

The main menu items are located in the left pane of the window at all times.

Figure 2-1 SGMI controls



Note: The wireless features do not appear in the SGMI until a compatible Symantec Gateway Security WLAN (Wireless Local Area Network) Access Point option is properly installed and configured. See the *Symantec Gateway Security 300/400 Series Wireless Implementation Guide* for more information.

Understanding left pane main menu options

The menu options in the left pane of the SGMI let you do the following:

Logging/Monitoring	Configure logging and monitoring functions. You can set up the size and rollover rate of the system log file and view current log files, archived log files, and current system status.
Administration	Configure administrative functions such as setting passwords, allowing remote management of the security gateway, specifying advanced management parameters, viewing trusted certificates, and scheduling LiveUpdate frequency.
LAN	Specify usable LAN IP and DHCP addresses and port assignments.
WAN/ISP	Specify network connection types, DNS settings, modem settings, and routing table information.
Firewall	Control the firewall functionality of the security gateway. You can set up inbound and outbound rules, enable system services, organize computer groups, map services to ports, and customize connectivity for internal network nodes.
Wireless	Control the wireless functionality supported by the security gateway.
VPN	Build and manage Virtual Private Network (VPN) tunnels to connect securely to remote users and gateways.
IDS/IPS	Manage the level of Intrusion Detection and Intrusion Prevention you want to provide to internal network nodes.
Antivirus Policy	Enable and manage antivirus protection for the security gateway and its protected network.
Content Filtering	Control allow or deny lists with which you can filter or block Web sites and URLs.

Understanding right pane features

The right-pane features include the following:

Menu tabs	For each left-pane menu option, there is a corresponding set of right-pane menu tabs that help break down the tasks associated with the menu item into logical groupings. For example, the Logging/Monitoring menu option contains the following tabs: ■ Status View system status, including network connectivity, physical addresses, and appliance version and model information. ■ View Log View the appliance log file. ■ Log Settings Set the parameters for viewing the appliance log file. ■ Troubleshooting Enable testing tools and debugging utilities.
Command buttons	Command buttons generally save, validate, or cancel changes you have to the right pane content. They vary with the left pane menu option selected.
Content	The right pane content consists of the group of fields within the menu tab selected. The valid entries in each of the fields are described in "Field descriptions" on page 117.
Help button	Clicking this button will open the help file to a page corresponding to the menu tab that is currently selected. You can then navigate to other help pages by clicking the Previous and Next buttons.

Tips for using the SGMI

The following list describes how to best work within the SGMI:

- To submit a form, click the appropriate button in the user interface rather than pressing Enter on your keyboard.
- If you submit a form and receive an error, click the Back button in your Web browser. This retains the data you entered.
- In IP address text boxes, press the Tab key on your keyboard to switch between boxes.
- If the appliance automatically restarts after you click a button to submit the form in the user interface, wait approximately one minute before attempting to access the SGMI again.

Managing administrative access

You manage administrative access by setting a password for the administrator, as well as defining the IP addresses of computers that are authorized to access the appliance from the WAN side.

You can also configure a range of IP addresses from which you can remotely manage the appliance. The administration user name is always admin.

Note: You must set the administration password before you have remote access to the SGMI.

Setting the administration password

The administration password provides secure access to the SGMI. Setting and changing the password periodically limits access to the SGMI to people who have been given the password. You must have installed the appliance and connected your browser to the SGMI to set the password. See the *Symantec Gateway Security 400 Series Installation Guide* for more information about setting up the appliance.

You can set or reset the administration password in a number of ways, including:

- Running the Setup Wizard
  The Setup Wizard will prompt you to change the password. The default password is password.
  See "Understanding the Setup Wizard" on page 27.
- In the SGMI, on the Administration > Basic Management tab
  See "To set the administration password" on page 19.
- Pushing Reset button on rear panel
  Resetting the appliance using the Reset button resets the password to password, resets the LAN IP address to 192.168.0.1, and enables the DHCP server.
  See "Resetting the appliance" on page 104.
- Connecting to the serial port
  Resetting the appliance through the serial console resets the password to password.
  See "Managing the security gateway using the serial console" on page 21.
- Flashing the appliance
  Reflashing the appliance with the app.bin version of the firmware resets the password to password.
  See "Upgrading firmware manually" on page 100.

Note: You should change the administration password on a regular basis to maintain a high level of security.

To set the administration password

See "Basic Management tab field descriptions" on page 121.

To configure a password

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the Basic Management tab, under Administration Password, in the admin's Password text box, type the password.
   Passwords are case-sensitive.
3. In the Verify Password text box, type the password again.
4. Click **Save**.

To manually reset the password

1. On the back of the appliance, press the reset button for 10 seconds.
2. Repeat the procedure to configure a password. See "To configure a password" on page 19.

Configuring remote management

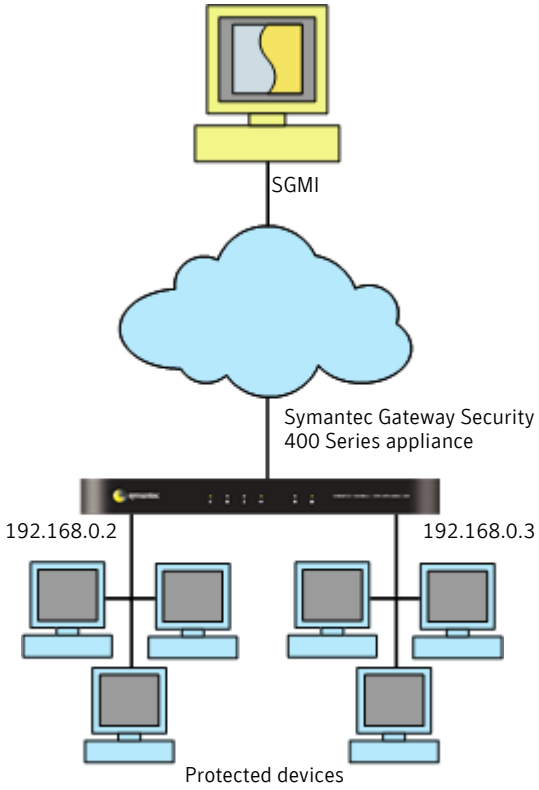
You can access the SGMI remotely, from the WAN, using a computer with an IP address that falls within a range of addresses set on the security gateway. The range is defined by a start and end IP address, which are configured in Administration > Basic Management > Remote Management in the SGMI. You should configure the IP addresses for remote management when you first connect to the SGMI. Remote management traffic is packaged and sent using the MD5 hash algorithm for security.

Note: For security reasons, you should perform all remote management through a VPN tunnel. This provides an appropriate level of security and confidentiality for your management session.

See "Establishing secure VPN connections" on page 65.

Figure 2-2 shows a remote management configuration.

Figure 2-2 Remote management



To configure remote management, specify both a start and end IP address. To remotely manage from only one IP address, type it as both the start and end IP address. The start IP address is the lower number in the range of IP addresses, and the end IP address is the higher number in the range of IP addresses. Leave these fields blank to deny remote access to the SGMI.

To configure remote management

See "Basic Management tab field descriptions" on page 121.

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the Basic Management tab, under Remote Management, in the Start IP Address text boxes, type the first IP Address (lowest in the range).
3. In the End IP Address text boxes, type the last IP Address (highest in the range).
   To permit only one IP address, type the same value in both text boxes. To prevent remote access, leave these fields blank.
4. To enable remote Trivial File Transfer Protocol (TFTP) upgrades to the appliance's firmware from the configured IP address range, check **Allow Remote Firmware Upgrade.**
   The default is disabled. See "Upgrading firmware manually" on page 100.
5. Click **Save**.
6. To access the SGMI remotely, browse to the <appliance IP address>:8088, where <appliance IP address> is the WAN IP address of the appliance.
   When you attempt to access the SGMI remotely, you must log in with the administration user name and password.

Managing the security gateway using the serial console

You can configure or reset the security gateway through the serial port using the null modem cable that is supplied with the security gateway. Configuring the security gateway from the serial console is useful when installing the appliance in an existing network, because it prevents the security gateway from interfering with the network when it is connected.

You can configure the following subset of settings through the serial console:

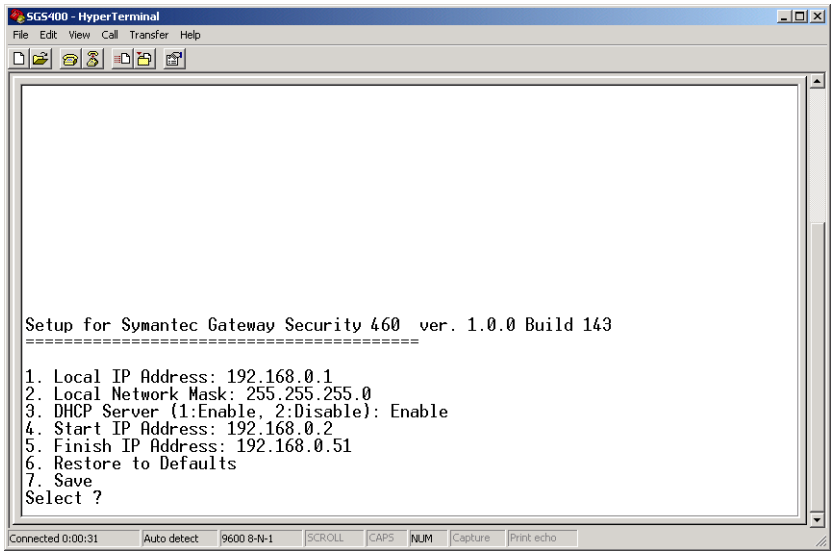
- LAN IP address (IP address of the security gateway)
- LAN network mask
- Enable or disable the DHCP server
- Range of IP addresses for the DHCP server to allocate

To manage the security gateway using the serial console

1. On the rear of the appliance, connect the null modem cable to the serial port.
2. Connect the null modem cable to your computer's COM port.
3. On the rear of the appliance, turn DIP switch 3 to the on position (up).
4. On your keyboard, ensure that the Scroll Lock is not on.
5. Run a terminal program, such as HyperTerminal.
6. In the terminal program, set the program to connect directly to the COM port on your computer to which the appliance is physically connected.
7. Set the communication settings as follows:

Baud (Bits per second)	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

8. Connect to the appliance.



9 After the terminal session has been established, on the rear panel of the appliance, quickly press the reset button.

10 At the Select? prompt, do one of the following:

Local IP Address	Type 1 to change the IP address of the appliance.
Local Network Mask	Type 2 to change the netmask of the appliance.
DHCP Server	Type 3 to enable or disable the DHCP server feature of the appliance.
Start IP Address	Type 4 to specify the first IP address in the range that the DHCP server can allocate.
Finish IP Address	Type 5 to specify the last IP address in the range that the DHCP server can allocate.
Restore to Defaults	Type 6 to restore the appliance's default settings for Local IP address, local network mask, DHCP server, and DHCP range.

For example, if you are changing just the local IP address and local network mask, do the following:

- Type 1.
- Type the new IP address.
- Type 7 to save the IP address.
- Type 2.
- Type the new netmask.
- Type 7 to save the netmask.
- Press Enter.

Or, to restore the default values for the appliance, press Enter.

11 Type **7**.
The appliance restarts.

12 On the rear of the appliance, turn DIP switch 3 to the off position (down).

13 On the rear of the appliance, quickly press the reset button.

Chapter 3

Configuring a connection to the outside network

This chapter includes the following topics:

- About connecting to the outside network
- Network examples
- Understanding the Setup Wizard
- About dual-WAN port appliances
- Understanding connection types
- Configuring connectivity
- Configuring advanced connection settings
- Configuring dynamic DNS
- Configuring routing
- Configuring advanced WAN/ISP settings

About connecting to the outside network

The Symantec Gateway Security 400 Series WAN/ISP functionality lets you configure connections to the outside world. This can be the Internet, a corporate network, or any other external private or public network. WAN/ISP functionality can also be configured to connect to an internal LAN when the appliance is protecting an internal subnet. Configure the WAN connections as soon as you install the appliance.

You can configure or change the appliance's connectivity on the WAN ports using the Setup Wizard or the WAN/ISP windows. The Setup Wizard is run automatically the first time you access the appliance after you complete the hardware installation.

Before you start configuring a WAN connection, determine what kind of connection you have to the outside network, and based on the connection type, gather information to use during the configuration procedure. See the *Symantec Gateway Security 400 Series Installation Guide* for worksheets to help you plan the configuration process.

Symantec Gateway Security 400 Series models 420 and 440 have one WAN port to configure. Models 460 and 460R appliances have two WAN ports that you can configure separately and differently depending on your needs. Some settings apply to both WAN ports, while other settings apply specifically to WAN1 or WAN2.

Warning: After you reconfigure WAN connections and restart the appliance, network traffic is temporarily interrupted. Once the appliance is restarted, VPN connections are automatically reestablished.

Network examples

This section describes the most common ways in which the Symantec Gateway Security 400 Series can be installed and deployed in your network.

Figure 3-1 shows a network diagram of a Symantec Gateway Security 400 Series connected to the Internet. The termination point represents any network termination type. This is a device that may be provided by your Internet Service Provider (ISP), or a network switch. The computer used for appliance management is connected directly to the appliance using one of the LAN ports on the appliance, and uses a browser to connect to the Security Gateway Management Interface (SGMI). The users within the protected network communicates through the Symantec Gateway Security 400 Series appliance to the Internet.

Figure 3-1 Connection to the Internet

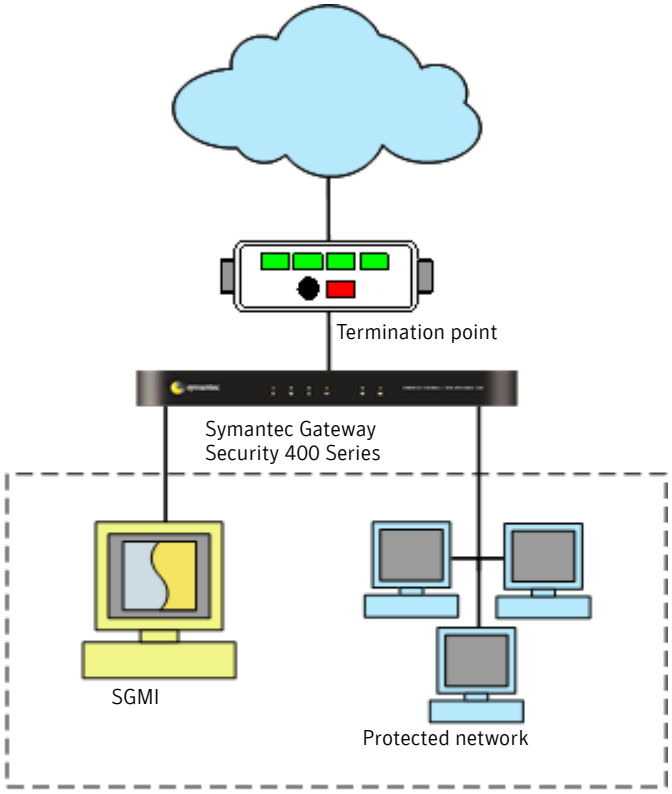


Figure 3-2 shows a network diagram of an appliance connecting to an intranet. In this scenario, the appliance protects an enclave of the larger internal network from unauthorized internal users. Enclave traffic from the protected network passes through the Symantec Gateway Security 400 Series appliance and through the Symantec Gateway Security 5400 Series appliance to the Internet.

Figure 3-2 Connection to an intranet

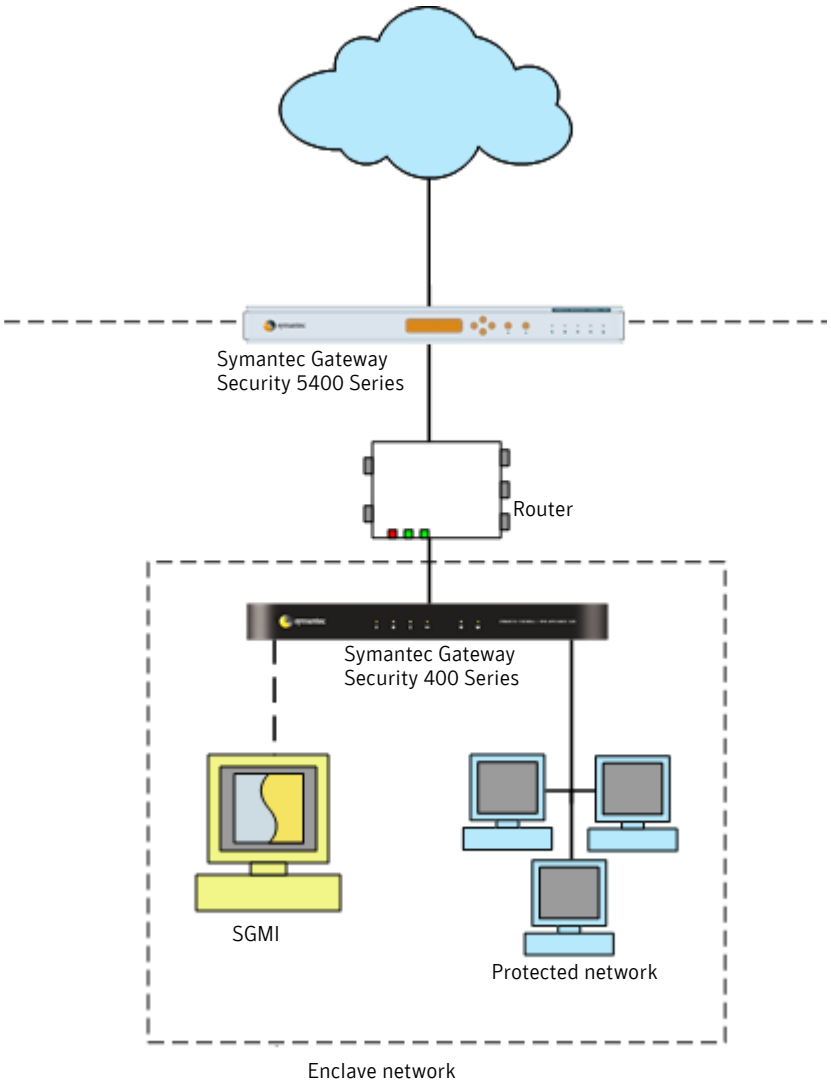


Figure 3-3 shows parallel subnets protected by two Symantec Gateway Security 400 Series appliances. In this scenario, each appliance protects its internal network from unauthorized internal users. Traffic from each protected network passes through the Symantec Gateway Security 400 Series to the Internet. One Symantec Gateway Security 400 Series is managed locally by the SGMI and the other is managed by the Symantec management console.

For details on managing with the Symantec management console, see the *Symantec Event Manager and Advanced Manager for Security Gateways (Group 2) v2.1 Administrator's Guide*.

Figure 3-3 Parallel networks

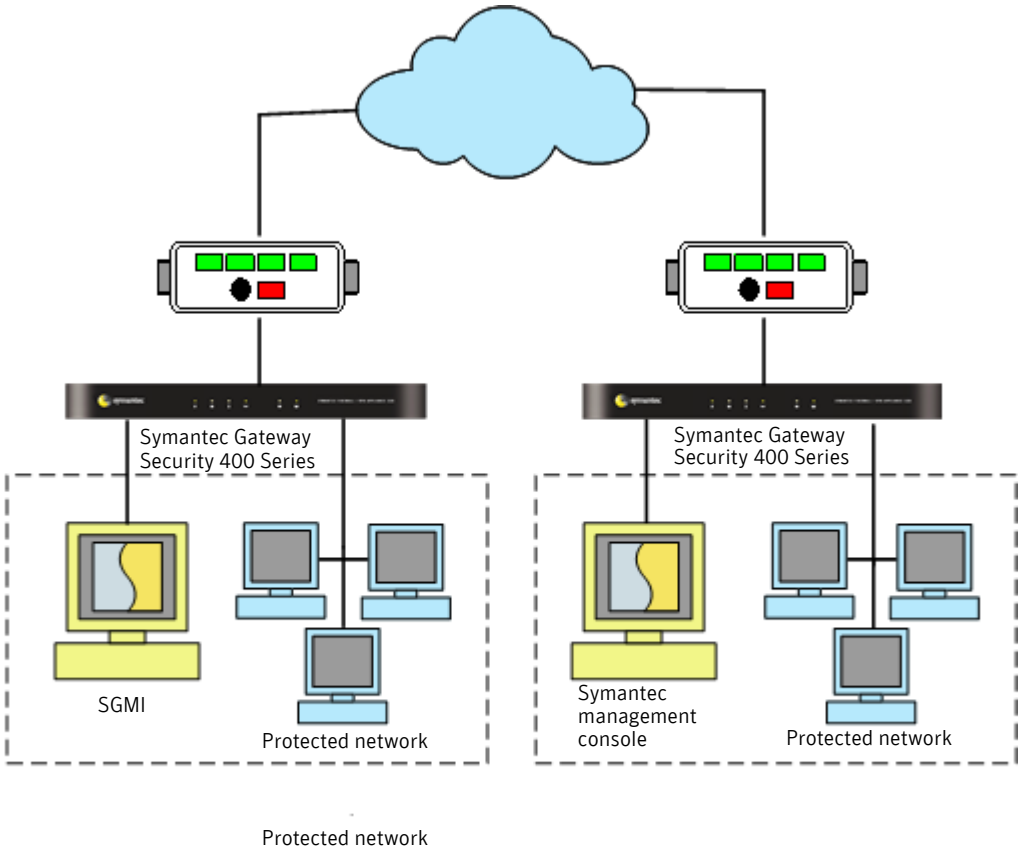
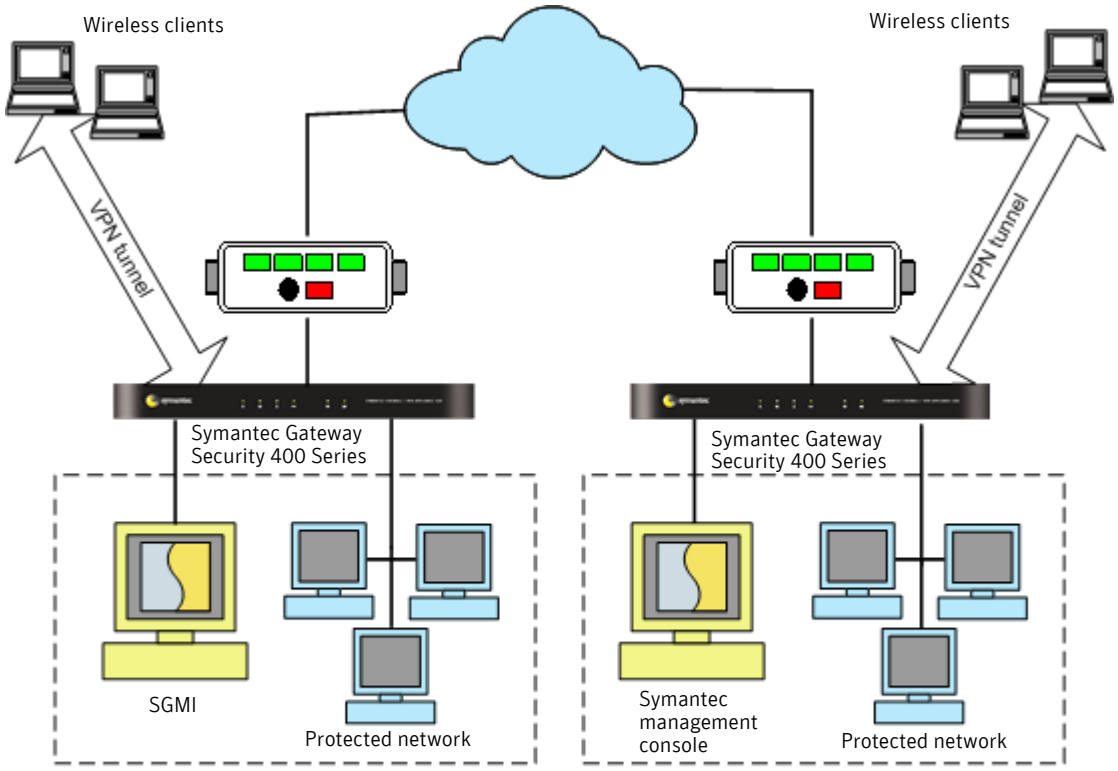


Figure 3-4 shows the addition of wireless clients, connecting to the Symantec wireless LAN card using VPN tunnels. In this scenario, each appliance protects its internal network and its wireless clients from unauthorized internal users. Traffic from the protected network passes through the Symantec Gateway Security 400 Series to the Internet. Again, one network is managed using SGMI and one using the Symantec management console.

For details on managing with the Symantec management console, see the *Symantec Event Manager and Advanced Manager for Security Gateways (Group 2) v2.1 Administrator's Guide.*

Figure 3-4 Network with wireless clients



Understanding the Setup Wizard

The Setup Wizard launches automatically the first time you browse to the appliance. The Setup Wizard helps you to configure basic connectivity to the Internet or an intranet.

The Setup Wizard verifies the current status of the WAN connection before proceeding. If the WAN port (called WAN 1 on model 460/460R) is connected to an active network, the Setup Wizard guides you through configuring LiveUpdate and setting the administrator password. If the WAN port is not currently active, the Setup Wizard guides you through entering your ISP-specific connection parameters. Later, for model 460/460R, use the WAN/ISP tab in the SGMI to configure WAN 2 or to configure advanced connection settings for either WAN port.

You can rerun the Setup Wizard at any time after the initial installation. To run the Setup Wizard, on the WAN/ISP tab > Main Setup window, click Run Setup Wizard. See the *Symantec Gateway Security 400 Series Installation Guide* for more information.

Note: To change the language in which the SGMI appears, rerun the Setup Wizard and select a different language.

Warning: Anything you type and save on the WAN/ISP tab overwrites what you entered previously in the Setup Wizard. This may cause a loss of WAN connectivity.

About dual-WAN port appliances

Symantec Gateway Security 400 Series models 460 and 460R appliances have two WAN ports, WAN 1 and WAN 2. Models 460 and 460R support different types of network settings on each of its WAN ports. For example, you may have a static IP account through your business as the primary WAN connection and a secondary (and less expensive) dynamic IP account for a backup connection. Each WAN port is treated as a completely different connection.

While some configurations apply to both WAN ports and for other configurations you must configure each WAN port separately. Table 3-1 describes WAN port configurations and whether you must configure one or both WAN ports.

Table 3-1 WAN port configurations

Configuration	WAN port	For more information
Connection types	Configure a connection type for each WAN port.	See "Understanding connection types" on page 29.
Backup account	You can configure a primary connection for WAN1 and then connect a modem to the serial port on the back of the appliance for a backup connection.	See "Dial-up accounts" on page 35.
Optional network settings	You can specify different configurations for each WAN port.	See "Optional network settings" on page 46.
Dynamic DNS	Applies to both WAN1 and WAN2.	See "Configuring dynamic DNS" on page 40.
DNS Gateway	Applies to both WAN1 and WAN2.	See "DNS gateway" on page 45.
Alive Indicator	Configure an alive indicator for each WAN port.	See "Dial-up accounts" on page 35 or "Configuring advanced WAN/ISP settings" on page 43
Routing	Configure routing for each WAN port.	See "Configuring routing" on page 42.
WAN port load balancing and bandwidth aggregation	Set the percentage of traffic you want sent through WAN1; the remainder goes through WAN2.	See "Load balancing" on page 44.
Bind SMTP	Bind SMTP to either WAN1 or WAN2.	See "SMTP binding" on page 44.
High availability	Specify whether high availability is used for each port.	See "High availability" on page 43.

Understanding connection types

To connect the appliance to an outside or internal network, you must understand your connection type.

First, determine if you have a dial-up or broadband account. Typical dial-up accounts are analog (through a normal phone line connected to an external modem) and ISDN (through a special phone line). Typical dedicated accounts are broadband cable, DSL, T1/E1, or T3 connected to a terminal adaptor.

Table 3-2 and Table 3-3 describe the supported connection types. including the following information:

- The Connection type column correlates to the option button you click on the Main Setup tab or in the Setup Wizard.
- The Services column defines the types of accounts or protocols that are associated with the connection type.
- The Network termination types column lists the physical devices that a particular connection type typically uses to connect to the Internet or a network.

Once you have determined your specific type of connection, refer to the appropriate configuration section later in this chapter.

Note: Connect only RJ-45 cables to the WAN ports.

Table 3-2 Dial-up connection types

Connection type	Services	Network termination types
Analog or ISDN	Plain Old Telephone Service (POTS)	Analog dial-up modem
	Integrated Services Digital Network (ISDN)	Digital dial-up modem An ISDN modem is sometimes called a terminal adaptor.

If you have a dedicated account, refer to Table 3-3 to determine which connection type you have.

Table 3-3 Dedicated connection types

Connection type	Services	Network termination types
DHCP	Broadband cable	Cable modem
	Digital Subscriber Line (DSL)	DSL modem with Ethernet cable
	Direct Ethernet connection	Ethernet Cable (usually an enclave network)
PPPoE	PPPoE	ADSL modem with Ethernet cable
Static IP (Static IP & DNS)	Broadband cable	Cable modem
	Digital Subscriber Line (DSL)	DSL modem
	T1	Channel Service Unit/Digital Service Unit (CSU/DSU)
	Direct Ethernet connection	Ethernet cable (usually an enclave network)
PPTP	PPTP	DSL modem with Ethernet cable

Your ISP or network administrator may also be able to help you determine your connection type.

Configuring connectivity

Once you have determined your connection type, you can configure the appliance to connect to the Internet or intranet using the settings appropriate for that connection.

DHCP

Dynamic Host Configuration Protocol (DHCP) automates the network configuration of computers. It lets a network with many clients extract configuration information from a single DHCP server. In the case of a dedicated Internet account, the users are the clients extracting information from the ISP's DHCP server, and IP addresses are only assigned to connected accounts.

Your ISP account may use DHCP to allocate IP addresses. Account types that frequently use DHCP are broadband cable and DSL. ISPs may authenticate broadband cable connections using the MAC (physical) address of your computer or gateway.

Before configuring DHCP for your WAN ports, you must select DHCP (Auto IP) as your connection type on the Main Setup window.

To configure DHCP

See "Main Setup tab field descriptions" on page 128.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. For models 420 and 440, do the following:
   - In the right pane, on the Main Setup tab, under Connection Type, click **DHCP**.
   - Click **Save**.
3. For models 460 and 460R, do the following:
   - To select a connection type for WAN1, under WAN1 (External), in the Connection Type drop-down list, click **DHCP**.
   - To select a connection type for WAN2, under WAN2 (External), in the Connection Type drop-down list, click **DHCP**.
4. Click **Save**.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is used by many Asymmetrical Digital Subscriber Line (ASDL) providers. It is a specification for connecting many users on a network to the Internet through a single dedicated medium, such as a DSL account.

You can specify whether to connect or disconnect your PPPoE account manually or automatically. This is useful to verify connectivity.

You can configure the appliance to connect only when an Internet request is made from a user on the LAN (for example, browsing to a Web site) and disconnect when the connection is idle (unused). This feature is useful if your ISP charges on a per-usage time basis.

You can use multiple logins (if your ISP account allows multi-session PPPoE) to obtain additional IP addresses for the WAN. These are called PPPoE sessions. The login may be the same user name and password as the main session or may be different for each session, depending on your ISP. Up to five sessions or IP addresses are allowed for models 420 and 440 and up to three sessions for each WAN port on models 460 and 460R. LAN hosts are bound to a session on the Computers tab in the SGMI.

See "Configuring LAN IP settings" on page 49.

Note: Multiple IP addresses on a WAN port are only supported for PPPoE connections.

By default, all settings are associated with Session 1. For multi-session PPPoE accounts, configure each session individually. If you have multiple PPPoE accounts, assign each one to a different session in the SGMI.

Before configuring the WAN ports to use a PPPoE account, gather the following information:

- User name and password
  All PPPoE accounts require user names and passwords. Get this information from your ISP before configuring PPPoE.
- Static IP address
  You may have purchased or are assigned a static IP address for the PPPoE account.

To configure PPPoE

See "PPPoE tab field descriptions" on page 129.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. For models 420 and 440, do the following:
   - In the right pane, on the Main Setup tab, under Connection Type, click **PPPoE**.
   - Click **Save**.
3. For models 460 and 460R, do the following:
   - In the right pane, on the Main Setup tab, under WAN1 (External), in the Connection Type drop-down list, click **PPPoE (xDSL)**.
   - To use WAN 2, under WAN 2 (External), under HA Mode, click **Normal**.
   - To use WAN2, under WAN2 (External), in the Connection Type drop-down list, click **PPPoE (xDSL)**.
   - On the WAN Port drop-down list, select a WAN port to configure.
   - Click **Save**.
4. If you have a multi-session PPPoE account, under WAN Port and Sessions, on the PPPoE Session drop-down list, select the appropriate session.
   If you have a single-session PPPoE account, leave the PPPoE session at Session 1.
5. Under Connection, check **Connect on Demand**.
   To connect to a PPPoE session manually, uncheck **Connect on Demand**, and then under Manual Control, click **Connect**.
6. In the Idle Time-out text box, type the number of minutes of inactivity after which you want the appliance to disconnect from the PPPoE account.
7. If you have a static IP PPPoE Internet account, in the Static IP Address text box, type the IP address. Otherwise, leave the value at 0.
8. Under Choose Service, click **Query Services.**
   You must be disconnected from your PPPoE account to use this feature. See "Connecting manually to your PPTP account" on page 35.
9. From the Service drop-down list, select a PPPoE service.
   You must click Query Services to select a service.
10. In the User Name text box, type your PPPoE account user name.
11. In the Password text box, type your PPPoE account password.
12. In the Verify Password text box, retype your PPPoE account password.
13. Click **Save**.

Verifying PPPoE connectivity

Once the appliance is configured to use the PPPoE account, verify that it connects correctly.

To verify connectivity

See "PPPoE tab field descriptions" on page 129.

See "Status tab field descriptions" on page 118.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. In the right pane, on the PPPoE tab, under Manual Control, click **Connect**.
3. In the left pane, click **Logging/Monitoring**.

In the right pane, on the Status tab, under WAN1 (External Port), the connection status is displayed.

If you are not connected, verify the following items:

- Your user name and password are correct. Some ISPs expect the user name to be in email address format, for example, johndoe@myisp.net.
- Check that all the cables are firmly plugged in.
- Verify your account information with your ISP and check that your account is active.

Connecting manually to your PPPoE account

You can manually connect or disconnect from your PPPoE account. For models 460 and 460R, you can manually control the connection for either WAN port. This is useful to troubleshoot the connection to the ISP.

To manually control your PPPoE account

You can manually control your PPPoE account through the SGMI.

See "PPPoE tab field descriptions" on page 129.

To manually connect to the PPPoE account

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. For models 420 and 440, in the right pane, on the PPPoE tab, under Manual Control, click **Connect**.
3. For models 460 and 460R, do the following:
   - In the right pane, on the PPPoE tab, under WAN Port and Sessions, in the WAN Port drop-down list, select the WAN port to connect.
   - In the Session drop-down list, select a PPPoE session.
   - Under Manual Control, click **Connect**.

To manually disconnect from the PPPoE account

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. For models 420 and 440, in the right pane, on the PPPoE tab, under Manual Control, click **Disconnect**.
3. For models 460 and 460R, do the following:
   - In the right pane, on the PPPoE tab, under WAN Port and Sessions, in the WAN Port drop-down list, select the WAN port to disconnect.
   - In the Session drop-down list, select a PPPoE session.
   - Under Manual Control, click **Disconnect**.

Static IP and DNS

When you establish an account with an ISP, you may have the option to purchase a static (permanent) IP address. This lets you run a Web or FTP server, because the address remains the same all of the time. Any type of account (dial-up or dedicated) can have a static IP address.

The appliance forwards DNS lookup requests to the specified DNS server for name resolution. The appliance supports up to three DNS servers. When you specify multiple DNS servers, they are used in sequence. After the first server is used, the next request is forwarded to the second server and so on.

If you have a static IP address with your ISP or are using the appliance behind another security gateway, select Static IP and DNS for your connection type. You can specify your static IP address and the IP addresses of the DNS servers you want to use for name resolution.

Before configuring the appliance to connect with your static IP account, gather the following information:

- Static IP address, netmask, and default gateway addresses
  Contact your ISP or IT department for this information.
- DNS addresses
  You must specify the IP address for at least one, and up to three, DNS servers. Contact your ISP or IT department for this information. You do not need DNS IP address entries for dynamic Internet accounts or accounts where a DHCP server assigns the IP addresses.
  If you have a static IP address with PPPoE, configure the appliance for PPPoE.

To configure static IP

See "Static IP & DNS tab field descriptions" on page 129.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. In the right pane, on the Main Setup tab, under Connection Type, click **Static IP**.
3. Click **Save**.
4. For models 420 and 440, do the following:
   - In the right pane, on the Static IP & DNS tab, under WAN IP, in the IP Address text boxes, type the desired IP address of the external (WAN) side of the appliance.
   - In the Network Mask text box, type the network mask.
     Change this only if required by your ISP.
   - In the Default Gateway text box, type the IP address of the default security gateway.
   - In the Domain Name Servers text boxes, type the IP address for at least one, and up to three, domain name servers.
   - Click **Save**.
5. For models 460 and 460R, do the following:
   - Under WAN1 (External), in the Connection Type drop-down list, click **Static IP**.
   - To use WAN 2, under WAN 2 (External), under HA Mode, click **Normal**.
   - To use WAN 2, under WAN2 (External), in the Connection Type drop-down list, click **Static IP**.
   - Click **Save**.
   - In the right pane, on the Static IP & DNS tab, under either WAN 1 IP or WAN2 IP, in the IP Address text boxes, type the desired IP address of the external (WAN) side of the appliance.
   - In the Network Mask text box, type the network mask.
   - In the Default Gateway text box, type the IP address of the default security gateway.
     The appliance sends any packet it does not know how to route to the default security gateway.
   - In the Domain Name Servers text boxes, type the IP address for at least one, and up to three, domain name servers.
6. Click **Save**.

PPTP

Point-to-Point-Tunneling Protocol (PPTP) is a protocol that enables secure data transfer from a client to a server by creating a tunnel over a TCP/IP-based network. Symantec Gateway Security 400 Series appliances act as a PPTP access client (PAC) when you connect to a PPTP Network Server (PNS), generally with your ISP.

Before beginning PPTP configuration, gather the following information:

- PPTP server IP address
  IP address of the PPTP server at the ISP.
- Static IP address
  IP address assigned to your account.
- Account information
  User name and password to log in to the account.

To configure PPTP

See "PPTP tab field descriptions" on page 132.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. For models 420 and 440, do the following:
   - In the right pane, on the Main Setup tab, under Connection Type, click **PPTP**.
   - Click **Save**.
3. For models 460 and 460R, do the following:
   - Under WAN1 (External), in the Connection Type drop-down list, click **PPTP**.
   - To use WAN 2, under WAN 2 (External), under HA Mode, click **Normal**.
   - To use WAN 2, under WAN2 (External), in the Connection Type drop-down list, click **PPTP**.
   - Click **Save**.
4. In the right pane, on the PPTP tab, under Connection, check **Connect on Demand.**
5. In the Idle Time-out text box, type the number of minutes of inactivity after which you want the appliance to disconnect the PPTP connection.
6. In the Server IP Address text box, type the IP address of the PPTP server.
7. If you have a static IP PPTP Internet account, in the Static IP Address text boxes, type the IP address. Otherwise, leave the value at 0.
8. Under User Information, in the User Name text box, type your ISP account user name.
9. In the Password text box, type your ISP account password.
10. In the Verify text box, type your ISP account password.
11. Click **Save**.

Verifying PPTP connectivity

Once the appliance is configured to use the PPTP account, verify that it connects correctly.

To verify PPTP connectivity

See "PPTP tab field descriptions" on page 132.

See "Status tab field descriptions" on page 118.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. For models 420 and 440, in the right pane, on the PPTP tab, under Manual Control, click **Connect**.

3 For models 460 and 460R, do the following:
   - In the right pane, on the PPTP tab, under WAN Port, in the WAN Port drop-down list, select the WAN port to connect.
   - Under Manual Control, click **Connect**.
4 In the left pane, click **Logging/Monitoring**.

In the right pane, on the Status tab, under WAN1 (External Port), the connection status is displayed.

If you are not connected, verify that you have typed your user name and password correctly. If you are still not connected, call your ISP and verify your account information and that your account is active.

Connecting manually to your PPTP account

You can manually connect to or disconnect from your PPTP account. For models 460 and 460R, you can manually control the connection for either WAN port. This is helpful for troubleshooting connectivity.

To manually connect to your PPTP account

For models 420 and 440, you can connect or disconnect to your PPTP account. For models 460 and 460R, you select the WAN port to control, and then connect or disconnect.

See "PPTP tab field descriptions" on page 132.

To manually connect your PPTP account

1 In the SGMI, in the left pane, click **WAN/ISP**.
2 For models 420 and 440, in the right pane, on the PPTP tab, under Manual Control, click **Connect**.
3 For models 460 and 460R, do the following:
   - In the right pane, on the PPTP tab, under WAN Port, in the WAN Port drop-down list, select the WAN port to connect.
   - Under Manual Control, click **Connect**.

To manually disconnect your PPTP account

1 In the SGMI, in the left pane, click **WAN/ISP**.
2 For models 420 and 440, in the right pane, on the PPTP tab, under Manual Control, click **Disconnect**.
3 For models 460 and 460R, do the following:
   - In the right pane, on the PPTP tab, under WAN Port, in the WAN Port drop-down list, select the WAN port to connect.
   - Under Manual Control, click **Disconnect**.

Dial-up accounts

There are two basic types of dial-up accounts: analog and ISDN. Analog uses a modem that connects to a regular telephone line (using an RJ-11 connector). ISDN is a digital dial-up account type that uses a special telephone line.

On the appliance, you can use a dial-up account as your primary connection to the Internet, or as a backup to your dedicated account. In backup mode, the appliance automatically dials the ISP if the dedicated connection fails. The appliance re-engages the dedicated account when it is stable; failover from the primary connection to the modem or from the modem to the primary connection can take 30 to 60 seconds.

You can configure a primary dial-up account and a backup dial-up account. You may configure a backup dial-up account if your primary dedicated account fails. First, you must connect the modem to the appliance. Then, you use the SGMI to configure the dial-up account.

You can also connect or disconnect your account manually at any time.

You must use an external modem for dial-up accounts. You connect the modem, both analog and ISDN, to the appliance through the serial port on the back of the appliance. Figure 3-5 shows the serial port on the rear panel of the models 420 and 440 appliances. Figure 3-6 shows the serial port on the rear panel of the models 460 and 460R appliances.

Figure 3-5 Rear panel of Symantec Gateway Security models 420 and 440 appliances

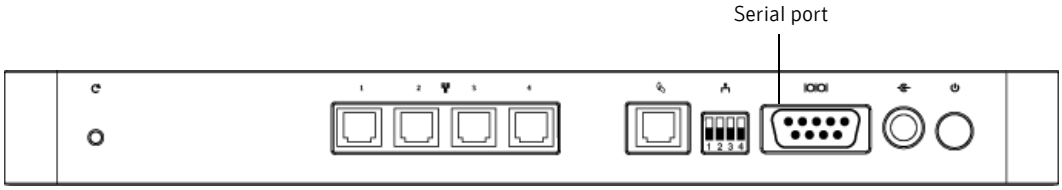
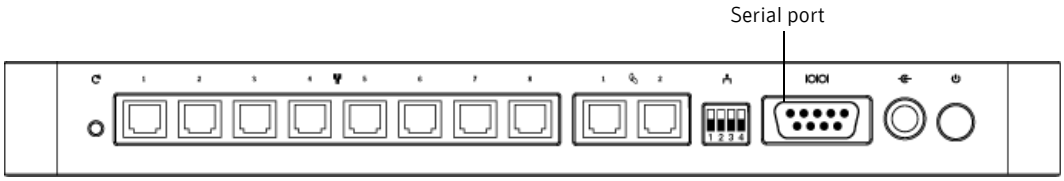


Figure 3-6 Rear panel of Symantec Gateway Security models 460 and 460R appliances



Before configuring the appliance to use your dial-up account as either the primary or backup connection, gather the following information and equipment:

Account information	User name, which may be different from your account name, and password for the dial-up account.
Dial-up numbers	At least one, and up to three, telephone numbers for the dial-up account.
Static IP address	Some ISPs assign static IP addresses to their accounts, or you may have purchased a static IP address.
Modem/cables	An external modem and a serial cable to connect the modem to the serial port on the back of the appliance.
Modem documentation	You may need to consult your modem's documentation for modem command or model information.

To configure dial-up accounts

First, you must connect the modem to the appliance. Then, you use the SGMI to configure the dial-up account.

Note: If your ISP gateway blocks ICMP requests such as PING, on the Main Setup tab, if you leave the Alive Indicator Site IP or URL text box blank, the appliance PINGs the default gateway to determine connectivity.

See "Dial-up Backup & Analog/ISDN tab field descriptions" on page 130.

To connect your modem

1. Plug one end of the serial cable into your modem.
2. Plug one end of the serial cable into the serial port on the back of the appliance.
3. If it requires external power, plug the modem into a wall socket.
4. Turn on the modem.

To configure your primary dial-up account

1. In the SGMI, in the left pane, click **WAN/ISP**.

2 In the right pane, on the Main Setup tab, under Connection Type, click **Analog/ISDN**.

3 Click **Save**.

4 On the Dial-up Backup & Analog/ISDN tab, under ISP Account Information, do the following:

User Name	Type the account user name.
Password	Type the account password.
Verify Password	Retype the account password.
Dial-up Telephone 1	Type the dial-up telephone number.
Dial-up Telephone 2	Optionally, type a backup dial-up telephone number.
Dial-up Telephone 3	Optionally, type a backup dial-up telephone number.

5 Under Modem Settings, do the following:

Model	Select the model of your modem.
Line Speed	Select the speed at which you want to connect.
Dial Type	Select the dial type.
Redial String	Type a redial string.
Initialization String	Type an initialization string. If you select a modem type other than Other, the initialization string is provided. If you select Other, you must type an initialization string.
Line Type	Select the type of telephone line.
Dial String	Type a dial string.
Idle Time Out	Type the amount of time, in minutes, after which the connection is closed if idle.

6 Click **Save**.

After you click Save, the appliance restarts. Network connectivity is briefly interrupted until the restart completes.

To enable the backup dial-up account

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Dial-up Backup and Analog/ISDN tab, under Backup Mode, do the following:

- Check **Enable Backup Mode**.
- In the Alive Indicator Site IP or URL text box, type the IP address or fully-qualified domain name of the site to check connectivity.

3 Under Modem Settings, click **Save**.

Controlling your dial-up account manually

You can force the appliance to connect or disconnect from your dial-up account. This is helpful for verifying connectivity.

To manually control the dial-up account

See "Dial-up Backup & Analog/ISDN tab field descriptions" on page 130.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 To connect to the dial-up account, on the Dial-up Backup & Analog/ISDN tab, under Manual Control, click **Dial**.

3 To disconnect from the dial-up account, on the Dial-up Backup & Analog/ISDN tab, under Manual Control, click **Hang Up**.

Verifying dial-up connectivity

Once you have configured the appliance to use your dial-up account, verify that it connects correctly.

If you are not connected, verify the following information:

- You have typed your user name and password correctly.
- Initialization string is correct for your model modem. Check your modem documentation for more information.
- Cables are securely plugged in.
- Phone jack to which the modem is connected is functioning.
- Verify your account information with your ISP and that your account is active.

To verify dial-up connectivity

See "Dial-up Backup & Analog/ISDN tab field descriptions" on page 130.

See "Status tab field descriptions" on page 118.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 In the right pane, on the Dial-up Backup & Analog/ISDN tab, under Manual Control, click **Dial**.

3 In the left pane, click **Logging/Monitoring**.

4 In the right pane, on the Status tab, under WAN1 (External Port), next to Connection Status, your connection status is displayed.

Monitoring dial-up account status

You can view and refresh the status of your dial-up account connection.

To monitor dial-up account status

See "Dial-up Backup & Analog/ISDN tab field descriptions" on page 130.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Dial-up Backup & Analog/ISDN tab, scroll to Analog Status.

3 To refresh the dial-up account status, on the Dial-up Backup & Analog/ISDN tab, under Modem Settings, click **Refresh**.

Configuring advanced connection settings

Advanced connection settings let you control your connectivity parameters more closely. If you have a DHCP connection, you can configure the renew settings. For PPPoE accounts, you can configure echo requests. For all connection types, you can specify packet size by setting the Maximum Transfer Unit (MTU).

Advanced DHCP settings

If you selected DHCP as your connection type, you can instruct the appliance to send a renew request, which tells the ISP to allocate a new IP address to the appliance.

You can tell the appliance at any time to request a new IP address by forcing a DHCP renew. However, you should only do this if requested by Symantec Technical Support.

To configure advanced DHCP settings

You can configure the idle renew time and manually force a DHCP renew request.

See "Advanced tab field descriptions" on page 136.

To configure idle renew time

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. On the Advanced tab, under Optional Connection settings, in the Idle Renew DHCP text box, type the number of minutes after which a renew lease request is sent.
3. Click **Save**.

To force a DHCP renew

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. For models 420 and 440, on the Advanced tab, under Optional Connection settings, click **Force Renew**.
3. For models 460 and 460R, do one of the following:
   - To renew WAN1, on the Advanced tab, under Optional Connection Settings, click **Renew WAN1**.
   - To renew WAN2, on the Advanced tab, under Optional Connection Settings, click **Renew WAN2**.

Advanced PPP settings

You can configure the echo requests that the appliance sends to verify that the appliance is connected to the PPPoE account.

To configure PPP settings

See "Advanced tab field descriptions" on page 136.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. On the Advanced tab, under PPP settings, do the following:
   - In the Time-out text box, type the number of seconds before trying another echo request.
   - In the Retries text box, type the number of times for the appliance to attempt to reconnect.
3. Click **Save**.

Note: To reset the echo request settings, click Restore Defaults. This also resets the MTU number and the DHCP Idle Renew settings to their default values.

Maximum Transmission Unit (MTU)

You can specify the maximum size of the packets that arrive at and leave the appliance through the WAN port. This is useful if a computer or another appliance along the transmission path requires a smaller MTU. On models 460 and 460R, if you are configuring WAN1 and WAN2, you can set a different MTU for each port.

To specify MTU size

See "Advanced tab field descriptions" on page 136.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. In the right pane, on the Advanced tab, under Optional Connection Settings, in the WAN port text box, type the MTU size.

3 Click **Save**.

Note: To reset the MTU size, click Restore Defaults. This also resets the echo request information and the DHCP Idle Renew settings to their default values.

Configuring dynamic DNS

Symantec Gateway Security 400 Series can use a dynamic DNS service to map dynamic IP addresses to a domain name to which users can connect.

If you receive your IP address dynamically from your ISP, dynamic DNS services let you use your own domain name (mysite.com, for example) or their domain name and your subdomain to connect to your services, such as a VPN gateway, Web site, or FTP. For example, if you set up a virtual Web server and your ISP assigns you a different IP address each time you connect the server, your users can always access www.mysite.com.

The appliances support two types of dynamic DNS services: standard and TZO. You can configure either service by specifying account information, or you can disable dynamic DNS completely.

See the *Symantec Gateway Security 400 Series Release Notes* for the list of supported services.

When you create an account with TZO, your ISP sends you the following information to log in and use your account: key (password), email (user name), and domain. Gather this information before configuring the appliance to use TZO. For more information about TZO dynamic DNS, go to http://www.tzo.com.

To use standard service DNS, gather the following information:

- Account information
  User name (which may be different from the account name) and password for the dynamic DNS account.
- Server
  IP address or resolvable name of the dynamic DNS server. For example, members.dyndns.org.

To configure dynamic DNS

For models 420 and 440, you can configure the WAN port to use dynamic DNS. For models 460 and 460R, you can configure WAN1, WAN2, or both ports to use dynamic DNS.

See "Dynamic DNS tab field descriptions" on page 133.

See "Main Setup tab field descriptions" on page 128.

To configure TZO dynamic DNS

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Dynamic DNS tab, under Service Type, click **TZO**.

3 Do one of the following:
   - For models 420 and 440, skip to step 4.
   - For models 460 and 460R, in the WAN Port drop-down list, select the WAN port for which you are configuring TZO.

4 Under TZO Dynamic DNS Service, do the following:
   - In the Key text box, type the key that TZO sent when the account was created.
   - In the Email text box, type the email address you specified when you created the TZO account.
   - In the Domain text box, type the domain name that TZO handles. For example, marketing.mysite.com.

5 Click **Save**.

To configure standard service DNS

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Dynamic DNS tab, under Service Type, click **Standard**.

3 Do one of the following:

- For models 420 and 440, skip to step 4.
- For models 460 and 460R, in the WAN Port drop-down list, select the WAN port for which you are configuring dynamic DNS.

4 Under Standard Service, do the following:

User Name	Type the dynamic DNS account user name.
Password	Type the dynamic DNS account password.
Verify Password	Retype the dynamic DNS account password.
Server	Type the IP address or DNS-resolvable name for the dynamic DNS server.
Host Name	Type the host name that you want to use.

5 Optionally, under Standard Optional Settings, do the following:

- To access your network with *.yourhost.yourdomain.com, where * is a CNAME like FTP or www, yourhost is the host name, and yourdomain.com is your domain name, check **Wildcards**.
- To use a backup mail exchanger, check **Backup MX**.
- In the Mail Exchanger text box, type the domain name of the mail exchanger.

6 Click **Save**.

Forcing dynamic DNS updates

When you force a dynamic DNS update, the appliance sends its current IP address, host name, and domain to the service. Do this only if requested by Symantec Technical Support.

For models 420 and 440, you can force a dynamic DNS update for the WAN port. For models 460 and 460R, you can force a dynamic DNS update for WAN1, WAN2, or both ports.

To force a DNS update

See "Dynamic DNS tab field descriptions" on page 133.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 For models 420 and 440, on the Dynamic DNS tab, under Service Type, click **Update**.

3 For models 460 and 460R, do the following:

- On the Dynamic DNS tab, under Service Type, in the WAN Port drop-down list, select the WAN port for which you are configuring TZO.
- Click **Update**.

Disabling dynamic DNS

You can disable dynamic DNS if you are hosting your own domain. On model 460 or 460R, you can disable dynamic DNS for both WAN ports.

To disable dynamic DNS

See "Dynamic DNS tab field descriptions" on page 133.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 For models 420 and 440, on the Dynamic DNS tab, under Service Type, click **Disable**.

3 For models 460 and 460R, do the following:

- On the Dynamic DNS tab, under Service Type, in the WAN Port drop-down list, select the WAN port to disable.
- Click **Disable**.

4 Click **Save**.

Configuring routing

If you install Symantec Gateway Security 400 Series appliances on a network with more than one directly connected router, you must specify to which router to send traffic. The appliance supports two types of routing: dynamic and static. Dynamic routing chooses the best route for packets and sends the packets to the appropriate router. Static routing sends packets to the router you specify. Routing information is maintained in a routing table.

Dynamic routing is administered using the RIP v2 protocol. When it is enabled, the appliance listens and sends RIP requests on both the internal (LAN) and external (WAN) interfaces. RIP v2 updates the routing table based on information from untrusted sources, so you should only use dynamic routing for intranet or department gateways where you can rely on trusted routing updates.

Routing helps the flow of traffic when you have multiple routers on a network. Configure dynamic or static routing to fit your needs.

Enabling dynamic routing

You do not need routing information to use dynamic routing.

To enable dynamic routing

See "Routing tab field descriptions" on page 134.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Routing tab, under Dynamic Routing, check **Enable RIP v2**.

3 Click **Save**.

Configuring static route entries

Before adding static routing entries to the routing table, gather the destination IP, netmask, and gateway addresses for the router to which you want traffic to be routed. Contact your IT department for this information.

You can add new route entries, edit existing entries, delete entries, or view a table of entries.

Note: If NAT is enabled, only six routes display in Routing List. When NAT is disabled, all configured routes appear in the list.

To configure static route entries

You can add, edit, or delete a static routing entry, or view the list of existing entries.

See "Routing tab field descriptions" on page 134.

To add a route entry

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Routing tab, under Static Routes, do the following:

Destination IP	Type the IP address to which to send packets.
Netmask	Type the net mask of the router to which to send packets.
Gateway	Type the IP address of the interface to which packets are sent.
Interface	Select the interface from which traffic is sent.
Metric	Type a number to represent the order in which you want the entry evaluated. For example, to evaluate the entry third, type 3.

3 Click **Add**.

To edit a route entry

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Routing tab, under Static Routes, in the Route Entry drop-down list, select a route entry.

3 Under Static Routes, change information in any of the fields.

4 Click **Update**.

To delete a route entry

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Routing tab, under Static Routes, in the Route Entry drop-down list, select an entry.

3 Click **Delete**.

To view the routing list table

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Routing tab, scroll to the bottom of the page.

Configuring advanced WAN/ISP settings

You can set advanced connectivity settings such as a DNS gateway, high availability/load balancing (HA/LB), SMTP binding, and failover. You can also set optional network settings, which identify the appliance to a network.

Note: Models 420 and 440 appliances have one WAN port, and do not support high availability, load balancing, and bandwidth aggregation.

High availability

On dual-WAN port appliances, you can configure each WAN port to failover to the other in the case of line connection failure.

You can configure high availability for each WAN port in one of three ways: Normal, Off, or Backup. Table 3-4 describes each mode.

Table 3-4 High availability modes

Mode	Description
Normal	Load balancing settings apply to the port when it is enabled and operational.
Off	WAN port is not used at all.

Table 3-4 High availability modes (Continued)

Mode	Description
Backup	WAN port only passes traffic if the other WAN port is not functioning.

By default, WAN1 is set to Normal and WAN2 is set to Off.

Bandwidth aggregation lets you combine the amount of traffic that goes over WAN1 and WAN2 to increase the amount of bandwidth your clients can use. For WAN data transfer, data aggregation can provide up to double the WAN throughput, depending on traffic characteristics. If you

To configure high availability

See "Main Setup tab field descriptions" on page 128.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 In the right pane, on the Main Setup tab, do the following:

- To configure the WAN1 port, under WAN1, select a high availability mode.
  The options are Normal, Off, and Backup. The default for WAN 1 is Normal.
- To configure the WAN2 port, under WAN2, select a high availability mode.
  The options are Normal, Off, and Backup. The default for WAN 2 is Backup.

3 Click **Save.**

Load balancing

Symantec Gateway Security 400 Series models 460 and 460R appliances each have two WAN ports. On these appliances, you can configure HA/LB between the two WAN ports.

You can set the percentage of packets that is sent over WAN1 or WAN2. You enter a percentage only for WAN1; the remainder of the packets are then sent over WAN2. If you have a slower connection, use a lower value for that WAN port for best performance.

To configure load balancing

See "Advanced tab field descriptions" on page 136.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Advanced tab, under Load Balancing, in the WAN 1 Load text box, type the percentage of traffic to pass through WAN 1.
The value in the WAN 2 (Calculated) % display is calculated automatically such that the sum of the two values is 100%.

3 Click **Save**.

SMTP binding

Use SMTP binding when you have two different Internet connections with different ISPs used over different WAN ports. It ensures that email sent by a client goes over the WAN port associated with your email server.

If the SMTP server is on the same subnet as one of the WAN ports, the security gateway automatically binds the SMTP server to that WAN port, and you do not have to specify the bind information.

To configure SMTP binding

See "Advanced tab field descriptions" on page 136.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Advanced tab, under Load Balancing, in the Bind SMTP with WAN Port drop-down list, select a binding option.

3 Under DNS Gateway, click **Save**.

Binding to other protocols

You can use the routing functionality of the firewall to bind other traffic. You add a static route to route traffic for the IP address of the destination server to a specific WAN port.

See "Configuring routing" on page 42.

Configuring failover

You can configure the appliance to periodically test the connectivity to ensure that your connection is available to your clients. After the amount of time that you specify (for example, 10 seconds), the appliance issues a PING command to the URL you specify as the Alive Indicator. If you do not specify an Alive Indicator, the default gateway is used.

Note: When selecting a URL to check, choose a fully-qualified domain name or IP address that you are sure will respond to a request, or you may receive a false positive when the connection is actually available.

When the WAN port on model 420 or 440 fails, the security gateway fails over to the serial port, which is connected to a modem. On model 460 or 460R, if one of the WAN ports fails, the security gateway fails over to the other WAN port. If both WAN ports fail, the security gateway fails over to the serial port.

If a line is physically disconnected, then the line is considered disconnected and the appliance attempts to route traffic to the serial port or the other WAN port.

If the cable is not physically disconnected, the appliance performs line checking every few seconds to determine if a line is active. If the line fails, it is shown as disconnected on the Logging/Monitoring > Status tab and an alternate route for traffic is attempted.

See "Dial-up accounts" on page 35 to configure failover for a dial-up account.

See "Connecting manually to your PPPoE account" on page 32 to configure a echo request for accounts that use PPP.

To configure failover

See "Main Setup tab field descriptions" on page 128.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 To configure an alive indicator for WAN1, on the Main Setup tab, under WAN1 (External), in the Alive Indicator Server text box, type the IP address or fully-qualified domain name of a server to which to send packets.

3 To configure an alive indicator for WAN2, on the Main Setup tab, under WAN2 (External), in the Alive Indicator Server text box, type the IP address or fully-qualified domain name of a server to which to send packets.

4 Click **Save**.

DNS gateway

You can specify a DNS gateway for local and remote name resolution over your VPN. For local and remote name resolution over VPN (gateway-to-gateway or client-to-gateway), the appliance can use a DNS gateway.

A backup DNS gateway can be specified. The DNS gateway handles name resolution, but should it become unavailable, the backup (generally a DNS gateway through your ISP) can take over.

To configure a DNS gateway

You can configure a primary and backup DNS gateway.

See "Advanced tab field descriptions" on page 136.

To configure a DNS gateway

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. On the Advanced tab, under DNS Gateway, in the DNS Gateway text boxes, type the IP address of the DNS gateway.
3. Click **Save**.

To configure DNS gateway backup

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. On the Advanced tab, under DNS Gateway, check **Enable DNS Gateway Backup**.
3. Click **Save**.

Optional network settings

Optional network settings identify your appliance to the rest of your network. If you plan to connect to or refer to your appliance by name, you must configure these settings.

Some ISPs authenticate by the MAC (physical) address of your Ethernet port. This is common with broadband cable (DHCP) services. You can clone your computer's adapter address to connect to your ISP with the Symantec Gateway Security 400 Series appliances. This is called MAC cloning or masking.

For models 420 and 440, you configure the settings for the WAN port. For models 460 and 460R, you can configure the network settings for one or both WAN ports.

Before you configure optional network settings, gather the following information:

Host name	Name of the appliance. For example, marketing.
Domain name	Name by which you address the appliance over the Internet. For example, mysite.com. If the host name is marketing, the appliance would be marketing.mysite.com.
MAC address	Physical address of the WAN of the appliance. If you are performing MAC cloning, get the MAC address that your ISP is expecting to see rather than the address of the appliance.

To configure optional network settings

See "Advanced tab field descriptions" on page 136.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. For models 420 and 440, do the following:
   - In the right pane, on the Main Setup tab, under Optional Network Settings, in the Host Name text box, type a host name.
     The host and domain names are case-sensitive.
   - In the Domain Name text box, type domain name for the appliance.
   - In the MAC Address text boxes, type the WAN network adapter address (MAC) that you are cloning.

3 For models 460 and 460R, do the following:

- To configure WAN1 or WAN 2, in the right pane, on the Main Setup tab, under Optional Network Settings, under WAN1 (External) or WAN 2 (External), do the following:

Host Name text box	Type a host name. The host and domain names are case-sensitive.
Domain Name text box	Type a domain name for the appliance
MAC Address text boxes	Type the WAN network adapter address (MAC) you are cloning.

4 Click **Save**.
After you click Save, the appliance restarts. Network connectivity is interrupted.

Chapter 4

Configuring internal connections

This chapter includes the following topics:

- Configuring LAN IP settings
- Configuring the appliance as a DHCP server
- Configuring port assignments

Configuring LAN IP settings

LAN settings let you configure your Symantec Gateway Security 400 Series appliance to work in a new or existing internal network.

Each appliance is assigned an IP address and netmask by default; you can change these settings at any time. This way, you can specify an IP address and netmask for the appliance that fits your existing network.

You can also configure the appliance to work as a DHCP server for LAN clients. This assigns IP addresses to the clients dynamically so that you do not have to configure each client to use a static IP address.

Note: Models 420 and 440 have four LAN ports, while models 460 and 460R have eight LAN ports. For each port, you must specify the port settings using the port assignments. These settings are used to configure secure wireless and wired LANs.

Each appliance has a default LAN IP address of 192.168.0.1 with a default network mask of 255.255.255.0. You can configure the appliance to use a different IP address and netmask for the LAN. This is useful if you want to configure a LAN to use a unique subnet for your network environment. For example, if your network already uses 192.168.0.x, you can change the appliance's IP address to 10.10.10.x, so you do not have to reconfigure your existing network.

Ensure that the IP address you choose for the appliance does not have zero (0) as the last octet.

You cannot set the appliance IP address to 192.168.1.0.

Note: After you change the appliance's LAN IP address, you must browse to the new appliance IP address to use the SGMI. If you click the Back button in the browser, it attempts to access the old IP address.

To configure LAN IP settings

See "LAN IP & DHCP tab field descriptions" on page 125.

1. In the SGMI, in the left pane, click **LAN**.
2. In the right pane, on the LAN IP & DHCP tab, under Unit LAN IP, in the IP Address text boxes, type the new IP address.
3. In the Network Mask text box, type the new network mask.
4. Click **Save**.

Configuring the appliance as a DHCP server

Dynamic Host Configuration Protocol (DHCP) allocates local IP addresses to computers on the LAN without manually assigning each computer its own IP address. This eliminates the need to have a static (permanent) IP address for each computer on the LAN and is useful if you have a limited number of IP addresses available. Each time a computer connected to the LAN is turned on, DHCP assigns it an IP address from the range of available addresses.

Note: Each client computer that you want to use DHCP must have its network configuration set to obtain its IP address automatically.

By default, the range of IP addresses that the appliance can assign is from 192.168.0.2 to 192.168.0.xxx, where xxx is the number of clients to support, plus two. For example, if you support 50 clients on your appliance, the last IP address in the range is 192.168.0.52. The DHCP server on the appliance serves IP addresses to up to 253 computers connected to it. If you change the IP address of the appliance, adjust the DHCP IP address range appropriately. See "Monitoring DHCP usage" on page 51.

Table 4-1 shows the default start and end IP addresses for each model. The default range is based on the recommended number of concurrent clients for each model. The number of clients you can support may vary depending on your traffic characteristics.

Table 4-1 Default DHCP IP address ranges

Model	Number of Clients	Start IP Address	End IP Address
420, 440	50	192.168.0.2	192.168.0.51
460, 460R	75	192.168.0.2	192.168.0.76

The DHCP server only supports class C networks. Class C networks have addresses from 192.0.0.0 through 223.255.255.0. The network number is the first three octets: 192.0.0 through 223.255.255. Each class C network can have one octet worth of hosts.

Note: You can place the appliance in any class network, but the DHCP server does not support this.

If you have a mix of clients that use DHCP and static IP addresses, the static IP addresses must be outside of the range of DHCP IP addresses. Also, you may want to assign static IP addresses to some services. For example, if you have a Web server on your site, you want to assign it a static IP address.

The DHCP server in the appliance is enabled by default. If you disable the DHCP server, each client connecting to the LAN must be assigned an IP address that is within the range. If you enable roaming on the appliance as a secondary wireless access point, the DHCP server is disabled.

To configure the appliance as a DHCP server

See "LAN IP & DHCP tab field descriptions" on page 125.

1. In the SGMI, in the left pane, click **LAN**.
2. In the right pane, on the LAN IP & DHCP tab, under DHCP, do one of the following:
   - To enable the appliance as a DHCP server, check **Enable**.
   - To disable the appliance as a DHCP server, check **Disable**.
3. In the Range Start IP text boxes, type the first IP address.
4. In the End IP text boxes, type the last IP address.
5. Click **Save**.

Monitoring DHCP usage

The DHCP Table lists the IP addresses that are assigned to connected clients. You can view the host name, IP address, physical address, and status for each client. This table takes up to one hour to fully update after the appliance has been rebooted.

To view DHCP usage

See "LAN field descriptions" on page 125.

- In the SGMI, in the left pane, click **LAN**.

Configuring port assignments

Port assignments on the security gateway let you specify if the LAN port resides on a trusted or untrusted network. Trusted ports are for networks not using VPN authentication to connect to the LAN. Untrusted ports are for wireless or wired networks using VPN clients to connect to LAN resources.

You can connect many network devices to the LAN ports: routers, switches, client machines, or other Symantec Gateway Security 400 Series appliances. For these options, select the standard port assignment. If you are connecting a Symantec Gateway Security 400 Series appliances that is configured as a wireless access point to a LAN port, you can secure the wireless connection using VPN technology. See the *Symantec Gateway Security 300/400 Series Wireless Implementation Guide*.

Once a port assignment is set, the untrusted ports enable and enforce encrypted VPN traffic, using global tunnels, to the appliance or using IPsec pass-thru to WAN-side endpoints.

Standard port assignment

When LAN ports are designated as standard, the appliance acts as a typical switch; it forwards traffic based on MAC address and traffic does not reach the security gateway engine unless it was specifically designated for it.

This option does not support client VPN tunnels terminating at the LAN. When a LAN port is set to standard, it is not considered part of the VLAN.

When you select standard, VPN traffic is not enforced at the switch; that is, a trusted private network is assumed.

SGS Access Point Secured port assignment

The SGS Access Point Secured port assignment enforces VPN security at the roaming access point or the switch level. This setting is used for connecting Symantec Gateway Security appliances.

Enforce VPN tunnels port assignment

The Enforce VPN tunnels/Allow IPsec pass-thru port assignment requires a VPN tunnel between a wireless VPN client and the security gateway. IPsec traffic is allowed to pass through a subsidiary switch with tunnel termination points located at the primary security gateway and the client.

To configure port assignments

You can set a specific LAN port to use a port assignment, or you can restore the default port settings.

See "Port Assignments tab field descriptions" on page 127.

To configure a port assignment

1 In the SGMI, in the left pane, click **LAN**.

2 In the right pane, on the Port Assignments tab, under Physical LAN Ports, from the Port numbers drop-down list, select a port assignment.

3 Click **Save**.

The appliance reboots when the port settings are saved.

To restore port assignment default settings

1 In the SGMI, in the left pane, click **LAN**.

2 In the right pane, on the Port Assignments tab, under Physical LAN Ports, click **Restore Defaults**.

The appliance reboots when the port settings are saved.

Chapter 5

Network traffic control

This chapter includes the following topics:

- Planning network access
- Understanding computers and computer groups
- Defining inbound access
- Defining outbound access
- Configuring services
- Configuring special applications
- Configuring advanced options

Planning network access

The Symantec Gateway Security 400 Series appliance includes firewall technology that lets you configure the firewall component to meet your security policy requirements. When configuring the firewall, identify all computers (nodes) to be protected on your network.

Note: This chapter uses the term computer to define anything that has its own IP address in the network; for example: a desktop PC, laptop, server, print server, terminal server, network photocopier, and so on.

Developing a security policy helps you to identify what you need to configure. See Appendix A in the *Symantec Gateway Security 400 Series Installation Guide*.

Before configuring the security gateway's firewall component, consider the following:

- Learn about computers and computer groups.
  See "Understanding computers and computer groups" on page 53.
- What kinds of users will be protected by the security gateway? Will all users have the same access and privileges?
- What types of services do you want to make available to internal users?
- What standard application services do you want to make available to external users?
- What types of special application services do you want to allow for external users and hosts?

Understanding computers and computer groups

Computers are nodes behind the appliance. This includes permanent resident desktops or laptops on the LAN, application servers, and any host or printer. You configure the appliance to recognize the computer by its MAC (physical) address.

Computer groups let you create outbound rules and apply them to computers who should have the same access. Instead of creating a traffic rule for each individual computer in your network, you define computer groups, assign each computer to a computer group, and then create rules for the group.

By default, all computers are part of the Everyone group and have no restrictions on Internet use until they are assigned to another computer group, which has traffic rules configured. You can create rules that apply to the Everyone group, or, for greater control, you can divide the computers into one of four computer groups, and then assign each group different rules. If a computer is not defined in the computers table, it belongs to the Everyone computer group.

Note: The security gateway has five computer groups: Everyone, Group 1, Group 2, Group 3, and Group 4. You cannot add, delete, or rename computer groups.

Before you create inbound and outbound rules to govern traffic, perform the following tasks in this order:

- Define the computer groups.
  See "Defining computer groups" on page 55.
- Define computers behind the appliance and assign them to computer groups.
  See "Defining computer group membership" on page 54.

Defining computer group membership

Defining computers is the first step in configuring the firewall component of the appliance.

When creating your security policy, leave the largest group of hosts in the Everyone computer group to minimize the input and management of MAC addresses. By default, all hosts belong to the Everyone computer group until you configure them to belong to one of the four other computer groups.

Review your security policy to determine how many computer groups you need (if any) and which users should be assigned to each computer group.

The Computers tab lets you identify each computer by typing its MAC address, assigning a static IP address, assigning it to a computer group, and binding it to a PPPoE session (if your ISP offers multiple PPPoE sessions). See "PPPoE" on page 30.

Note: To find the MAC address of a Microsoft Windows-based computer, at a DOS prompt, type ipconfig /all and look for the physical address.

On models 460 and 460R, you can restrict the computer to use only one of the WAN ports. This is useful if you have two broadband accounts, one on each WAN port, and you want a particular computer to use only one. This is useful for servers or applications that must always use a specific WAN IP address such as FTP. The default is disabled.

Defining computers

If you are using an ISP with PPPoE sessions, you bind a host to a session (WAN IP) on this tab.

Checking Reserved Host ensures that the DHCP server always offers the defined IP address to the computer you are defining, or you can set this IP address as a static address on the computer.

See "Computers tab field descriptions" on page 137.

To configure a new computer

1. In the left pane, click **Firewall**.
2. On the Computers tab, in the Host Name text box, type a host name.
3. In the Adapter (MAC) Address text box, type the address of the host's network interface card (NIC).

4 If the computer is an application server to which you want to allow access to an inbound rule, or to reserve an IP address for a computer that is not an application server, under Application Server, check **Reserved Host**.
See "Defining inbound access" on page 56.

5 In the IP Address text box, type the IP address of the host.

6 Under Computer Group, on the Computer Group drop-down list, select a group for your host to join.
The computer group properties are defined on the Firewall > Computer Groups tab.
See "Defining inbound access" on page 56.

7 Under Session Association - Optional, in the Bind with PPPoE Session drop-down list, select the session to bind to this host.
You must have a multi-session PPPoE account with your ISP if you want to bind a host to a PPPoE session. If you do not have an PPPoE account with your ISP, leave the Bind with PPPoE Session drop-down list at Session 1.

8 Click **Add.**

To verify that a host has been configured, you can check the Host List displayed at the bottom of the window. The fields in the list map to the fields entered when you configured the host.

Once you have finished adding computers to a computer group, you can configure the properties for each computer group on the Computer Groups tab in the SGMI.

To update an existing computer

1 In the left pane, click **Firewall**.

2 In the right pane, on the Computers tab, under Host Identity, in the Select Host drop-down list, select a host.

3 Make the changes to the computers fields.

4 Click **Update**.

The updated computer is displayed in the Host List.

To delete an existing computer

1 In the left pane, click **Firewall**.

2 In the right pane, on the Computers tab, under Host Identity, in the Select Host drop-down list, select a host.

3 Click **Delete**.

Defining computer groups

Computer groups are logical groups of network entities used for outbound rules. You must configure and bind all local hosts (nodes) to the computer group they are in using the Computers tab.

See "Defining computer group membership" on page 54.

You can configure the following properties for a computer group:

- Antivirus policy enforcement
See "How antivirus policy enforcement (AVpe) works" on page 81.
- Content filtering
See "Advanced network traffic control" on page 81.
- Access control
See "Defining inbound access" on page 56.

To define computer groups

See "Computer Groups tab field descriptions" on page 138.

1 In the left pane, click **Firewall**.

2 In the right pane, on the Computer Groups tab, under Security Policy, on the Computer Group drop-down list, select the computer group that you want to configure.

3 To enable AVpe, Under Antivirus Policy Enforcement, check **Enable AntiVirus Policy Enforcement,** and then click one of the following:

- Warn Only
- Block Connections

4 To enable content filtering, check **Enable Content Filtering**, and then select one of the following:

- Use Allow List
- Use Deny List

5 Under Access Control (Outbound Rules) select one of the following:

- No restrictions
- Block ALL outbound access
- Use rules defined in Outbound Rules Screen.
  See "Defining outbound access" on page 57.

6 Click **Save**.

Defining inbound access

Inbound rules control the type of traffic flowing into application servers on your appliance-protected networks. The default state for inbound traffic is that all traffic is denied (automatically blocked) until you configure inbound rules for each kind of traffic you want to allow. If the inbound traffic contains a protocol or application that is not part of an enabled rule, the connection request is denied and logged. The security gateway supports a maximum of 25 inbound rules.

When creating inbound rules, you must specify the applications server, the service, protocols, and ports that the rule allows, and source and destination information for each rule. When an inbound rule exists, any external host can successfully pass inbound traffic matching the rule.

Inbound rules redirect traffic that arrives on the WAN ports to another internal server on the protected LAN. For example, an inbound rule enabled for HTTP results in all HTTP traffic arriving on the WAN port to be redirected to the server specified as the HTTP application server. You must define the server before using it in a rule.

Inbound rules are not bound to a computer group.

To define inbound access

See "Inbound Rules field descriptions" on page 139.

To define a new inbound rule

1 In the SGMI, in the left pane, click **Firewall**.

2 To create a new rule, in the right pane, on the Inbound Rules tab, under Rule Definition, in the Name text box, type a unique name for the inbound rule.

3 Check **Enable Rule**.

4 In the Application Server drop-down list, select a defined computer.
Computers are defined on the Computers tab in the Firewall section. See "Computers tab field descriptions" on page 137.

5 On the Service drop-down list, select an inbound service.

6 Click **Add**.

To update an existing inbound rule

1 In the left pane, click **Firewall**.

2 In the right pane, on the Inbound Rules tab, in the Rule drop-down list, select an existing inbound rule.

3 Click **Select**.

4 Make the changes to the inbound rules fields.

5 Click **Update**.

To delete an inbound rule

1 In the left pane, click **Firewall**.

2 In the right pane, on the Inbound Rules tab, in the Rule drop-down list, select an existing inbound rule.

3 Click **Delete**.

Defining outbound access

By default, all computer groups are allowed outbound access. Also by default, all computers that you protect are in the Everyone computer group. When you define an outbound rule for a given computer group, and check the Use rules defined in Outbound Rules Screen check box, then all other traffic is blocked unless an outbound rule is defined to allow it. You must give each outbound rule a unique name.

You must also specify the type of traffic that the rule allows. Outbound rules let you define traffic to permit, rather than specifying traffic to deny or block. Once an outbound rule is added to the computer group, all other traffic is denied unless there is a specific rule to let it pass.

Following are the predefined outbound services:

- DNS
- FTP
- HTTP
- HTTPS
- Mail (SMTP)
- Mail (POP3)
- RADIUS Auth
- Telnet
- VPN IPSec
- VPN PPTP
- LiveUpdate
- SESA Server
- SESA Agent
- RealAudio1
- RealAudio2
- RealAudio 3
- PCA TCP
- PCA UDP

- TFTP
- SNMP

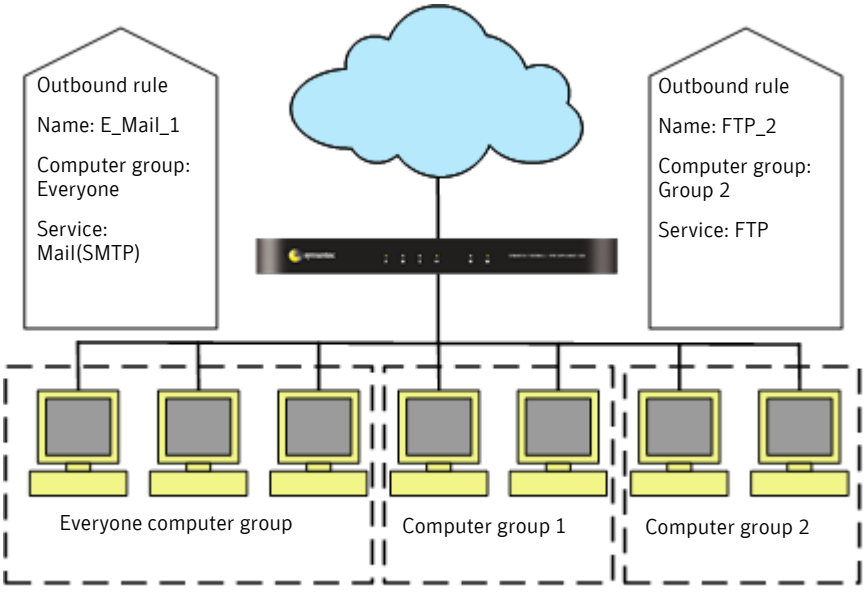
If you have services that are not on this list, or a service that does not use its default port, you can create your own custom services. You must create the custom services before creating the outbound rule.

See "Configuring services" on page 59.

Outbound rule example

As shown in Figure 5-1, an outbound rule enabled for FTP service for computer group 2 allows the members of computer group 2 outbound FTP service. An outbound rule enabled for Mail (SMTP) service for the Everyone computer group lets all members of the Everyone group send outbound email. An outbound rule enabled for FTP service for computer group 2 would allow the members of group 2 outbound FTP service. If computer group 1 has no rules, all outbound traffic is allowed by default.

Figure 5-1 Outbound rules example



Define outbound access

You can manage your outbound access by creating a rule, updating it when your needs change, or deleting it when you no longer need it. You can also temporarily disable outbound access for troubleshooting or controlling traffic.

See "Outbound Rules tab field descriptions" on page 140.

To define an outbound rule

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Outbound Rules tab, under Computer Groups, in the Computer Group drop-down list, select a computer group.
   To see a list of rules for the selected computer group, click **View**.
3. In the Name text box, type a unique name for the outbound rule.
4. Check **Enable Rule**.
5. On the Service drop-down list, select an outbound service.
6. Click **Add**.

To update an existing outbound rule

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Outbound Rules tab, under Computer Groups, on the Computer Group drop-down list, select a computer group.
   To see a list of rules for the selected computer group, click **View**.
3. In the Rule drop-down list, select an existing outbound rule.
4. Make the changes to the outbound rules fields.
5. Click **Update**.

To delete an outbound rule

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Outbound Rules tab, under Computer Groups, in the Computer Group drop-down list, select a computer group.
   To see a list of rules for the selected computer group, click **View**.
3. In the right pane, on the Outbound Rules tab, on the Rule drop-down list, select an existing outbound rule.
4. Click **Delete**.

Configuring services

You can define additional service applications used in inbound rules and outbound rules that are not already covered by the predefined services. You must configure these services before you can use them in any rules. The name of the service should identify the protocol or type of traffic that the rule allows.

You must specify the type of traffic and the destination server for that traffic. The type of traffic is selected from the list of predefined services and custom services.

Note: On models 460 and 460R, FTP application servers must be bound to a WAN port, WAN 1 or WAN 2. All other applications, such as HTTP, do not require binding to a WAN port.

See "Binding to other protocols" on page 45.

There are two types of protocols used by services: TCP and UDP. The port range specifies which port filter can communicate on the appliance. For protocols that allow for a port range, you must specify the listen on port starting and ending port numbers. For protocols that use a single port number, the listen on port starting and ending port numbers are the same.

Redirecting services

You can also configure services to be redirected from the ports they would normally enter (Listen on Port) to another port (Redirect to Port). Service redirection only applies to inbound rules. Outbound rules ignore this setting.

For example, to redirect inbound Web traffic entering on port 80 using TCP protocol, to an internal Web server listening for TCP on port 8080, you would create a new service application called WEB_8080. Select TCP as the protocol, and type 80 for both the listen on port starting and ending port numbers. For both the start and end redirect to ports, type 8080. Then create and enable an inbound rule for the Web application server that uses WEB_8080 as a service.

Note: Redirection port range sizes must be the same as the listen on port ranges. For example, if the listen on port range is 21 to 25, the redirection port range must also be four ports.

To redirect inbound traffic to the original destination port, leave the redirect fields blank.

Configuring a service

Create a service before you add it to an inbound rule. Once you create a service, you can update or delete it.

See "Services tab field descriptions" on page 140.

To configure a service

1. In the SGMI, in the left pane, click **Firewall**.
2. On the Services tab, under Application Settings, in the Name text box, type a name for the service that represents the application.
3. In the Protocol drop-down list, select **TCP** or **UDP**.
4. In the Listen on Port(s): Start text box, type a port number.
5. In the Listen on Port(s): End text box, type a port number.
6. In the Redirect to Port(s): Start text box, type a port number.
   Redirect only applies to inbound rules. If you are creating a service for an outbound rule, leave the Redirect to Port(s) text boxes blank.
   To redirect inbound traffic to the original destination port, leave the Redirect text boxes blank.
7. In the Redirect to Port(s): End text box, type a port number.
8. Click **Add**.

To update an existing service

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Services tab, on the Application drop-down list, select an existing service.
3. Make the changes to the services fields.
4. Click **Update**.

To delete a service

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Services tab, on the Application drop-down list, select an existing service.
3. Click **Delete**.

Configuring special applications

Special applications are used for dynamic port forwarding. To determine what ports and protocols an application needs for operation, consult the application's documentation for information on firewall or Network Address Translation (NAT) usage.

Some applications may need more than one entry defined and enabled; for example, when they have multiple port ranges in use. Special applications are global in scope and overwrite any computer group specific outbound rules or inbound rules. When enabled, the traffic specified can pass in either direction from any host.

Certain applications with two-way communication (such as games and video conferencing) need ports open in the firewall. Normally, you open ports with the Inbound Rules tab. But inbound rules only open ports for the application server IP address defined in its settings, because firewalls using NAT can only open a defined service for a single computer on the LAN (when using a single external IP).

The Special Applications tab works around this limitation by letting you set port triggers. The appliance listens for outgoing traffic on a range of ports from computers on the LAN and, if it sees traffic, it opens an

incoming port range for that computer. Once the communication is done, the appliance starts listening again so that another computer can trigger the ports to be opened for it.

Port triggers can be used very quickly (milliseconds), but for only one computer at a time. The speed with which port triggers are used gives the illusion of allowing multiple computers having the same ports opened.

Special Applications entries work best with applications that require low throughput. You may experience reduced performance with multiple computers activating streaming media or a heavy incoming or outgoing volume.

The appliance only listens for traffic on the LAN. The computer on the LAN activates the trigger, not traffic from the outside. The LAN application must initiate traffic and you must know the ports or range of ports it uses to set up a special applications entry. If traffic initiates from the outside, you must use an inbound rule.

Configuring a special application

Special applications help with dynamic packet forwarding. Configure a special application for two-way communication. You can then edit it or delete it as your needs change.

See "Special Applications tab field descriptions" on page 141.

To configure a special application

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Special Applications tab, under Select Applications, in the Name text box, type a name that represents the application.
3. Check **Enable**.
4. On the Outgoing Protocol drop-down list, select **TCP** or **UDP**.
5. In the Outgoing Port Range Start text box, type the first port number of the port range to listen on.
6. In the Outgoing Port Range End text box, type the last number of the port range to listen on.
7. In the Incoming Port Range Start text box, type the first port number in the range to open.
8. In the Incoming Port Range End text box, type the last port number in the range to open.
9. Click **Add**.

To update an existing special application

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Special Application tab, in the Special Application drop-down list, select an existing special application.
3. Make the changes to the special applications fields.
4. Click **Update**.

To delete an special application

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Special Applications tab, on the Application drop-down list, select an existing special application.
3. Click **Delete**.

Configuring advanced options

Symantec Gateway Security 400 Series has several advanced firewall options for special circumstances. These include:

- Enabling the IDENT port
- Disabling NAT mode
- Blocking ICMP requests
- Enabling WAN broadcast storm protection
- Enabling IPsec pass-thru
- Configuring an exposed host

Enabling the IDENT port

Queries to the TCP Client Identity Protocol (IDENT) port (113) normally result in the host name and company name information being returned. However, this service poses a security risk since attackers can use this information to hone in their attack methodology. By default, the appliance sets all ports to stealth mode. This configures a computer to appear invisible to those outside of the network. Some servers (like a certain email or Microsoft Internet Relay Chat (MIRC) servers) use the IDENT port of the system accessing them.

You can configure the appliance to enable the IDENT port. Enabling this setting makes port 113 closed (not open) and not stealth. You should enable this setting only if there are problems accessing a server (server time-outs).

Note: If you experience time-outs when using your mail (SMTP) service, enabling the IDENT port may correct this problem.

To enable the IDENT Port

See "Advanced tab field descriptions" on page 143.

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Advanced tab, under Optional Security Settings, check **Enable IDENT Port**.
3. Click **Save**.

Disabling NAT mode

You can configure the security gateway to work as a standard network router to separate different subnets on an internal network. Disabling NAT Mode disables the firewall security functions. This setting should only be used for intranet deployments where the security gateway is used as a bridge on a protected network. When the security gateway is configured for NAT mode, it behaves as a 802.1D (MAC bridge) device.

To disable NAT Mode

See "Advanced tab field descriptions" on page 143.

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Advanced tab, under Optional Security Settings, check **Disable NAT Mode**.
3. Click **Save**.

Blocking ICMP requests

You can configure the security gateway to drop and log any Internet Control Message Protocol (ICMP) redirect requests received on a WAN interface.

To block ICMP requests

See "Advanced tab field descriptions" on page 143.

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Advanced tab, under Optional Security Settings, next to Block ICMP Requests, do one of the following:
   - To block ICMP requests, click **Enable**.
   - To allow ICMP requests, click **Disable**.
3. Click **Save**.

Enabling WAN broadcast storm protection

Broadcast storm protection protects regular traffic from an overabundance of broadcast traffic. For example, a condition may exist in which a broadcast message results in many responses, each of which results in still more responses. This filter triggers when 63% of the WAN buffers are taken up by broadcast packets.

You may want to disable this feature to allow applications that require broadcast packets.

To enable WAN broadcast storm protection

See "Advanced tab field descriptions" on page 143.

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Advanced tab, under Optional Security Settings, next to WAN Broadcast Storm Protection, check **Enable**.
3. Click **Save**.

Enabling IPsec pass-thru

IPSec pass-thru is supported by the security gateway. If the VPN client used in Exposed Host has problems connecting from behind the security gateway, use the None setting.

The following list includes the supported IPsec types:

- 1 SPI
  ADI - Assured Digital
- 2 SPI (default)
  Standard (Symantec, Cisco Pix, and Nortel Contivity) clients
- 2 SPI-C
  Cisco Concentrator 30X0 Series clients
- Others
  Redcreek Ravlin
- None

Note: Only change the IPsec pass-thru setting if instructed to do so by Symantec Technical Support.

To configure IPsec pass-thru settings

See "Advanced tab field descriptions" on page 143.

1. In the SGMI, in the left pane, click **Firewall**.
2. On the Advanced tab, under IPsec Passthru Settings, select the IPsec types that you want to allow through the security gateway.
3. Click **Save**.

Configuring an exposed host

Exposed Host opens all ports so that one computer on a LAN has unrestricted two-way communication with Internet servers or users. This is useful for hosting games or special server applications.

All traffic that is not specifically allowed by inbound rules is directed to the exposed host.

Warning: Because of the security risk, activate Exposed Host only when required to do so.

To configure an exposed host

See "Advanced tab field descriptions" on page 143.

1. In the left pane, click **Firewall**.
2. In the right pane, on the Advanced tab, under Exposed Host, check **Enable Exposed Host**.
3. In the LAN IP Address text boxes, type the IP address of the host you want to expose.
4. In the Bind with WAN Port drop-down list (models 460 and 460R only), select the WAN port the exposed host is bound to.
   The default is WAN port 1.
5. In the Session drop-down list, select the session to bind to the exposed host.
6. Click **Save**.

Chapter 6

Establishing secure VPN connections

This chapter includes the following topics:

- How to use this chapter
- Creating security policies
- Identifying users
- Configuring gateway-to-gateway tunnels
- Configuring client-to-gateway VPN tunnels
- Monitoring VPN tunnel status

Virtual Private Networks (VPNs) let you securely extend the boundaries of your internal network and use insecure communication channels (such as the Internet) to safely transport sensitive data. VPNs let a single user or a remote network safely access the protected resources of another network.

Symantec Gateway Security 400 Series appliances support three types of VPN tunnels: gateway-to-gateway, client-to-gateway, and wireless client-to-gateway. To configure wireless client-to-gateway tunnels, see the *Symantec Gateway Security 300/400 Series Wireless Implementation Guide*.

Securing your network connections using VPN technology is an important step in ensuring the quality and integrity of your data. This section describes some key concepts and components you need to understand to configure and use the appliance's VPN feature.

VPN tunnels can also support dynamic and static gateway-to-gateway configurations, where tunnel parameters are created at each security gateway. Both ends must have the same parameters, including secret keys, security parameter indexes (SPIs), authentication schemes, and encryption methods.

How to use this chapter

Each section begins with an explanation of the feature it is describing (such as what a VPN policy is, how it works, and how you use it). If you are an experienced network or IT administrator, you may want to proceed directly to the latter half of the section for configuration instructions.

If you do not have significant network or IT experience or have never configured a security gateway (Symantec or otherwise), you should read the first half of each section before configuring the feature.

At the end of "Configuring gateway-to-gateway tunnels" on page 70 and "Configuring client-to-gateway VPN tunnels" on page 76, there are worksheets for you to fill out with the information you entered so that you may easily share connection information with your clients and remote gateway administrators.

Creating security policies

VPN tunnel negotiation occurs in two phases. In Phase 1, the Internet Key Exchange (IKE) negotiation creates an IKE security association with its peer to protect Phase 2 of the negotiation, which determines the protocol security association for the tunnel. For gateway-to-gateway connections, either security gateway can initiate Phase 1 or Phase 2 renegotiation at any time. Either security gateway can also specify intervals after which to renegotiate. For client-to-gateway connections, only the client can initiate Phase 1 or Phase 2 renegotiation. Phase 2 renegotiation is referred to as quick mode renegotiation.

Note: Symantec Gateway Security 400 Series does not support VPN tunnel compression. To create a gateway-to-gateway tunnel between a Symantec Gateway Security 400 Series appliance and a remote Symantec Gateway Security 5400 Series appliance or Symantec Enterprise Firewall, set the compression to NONE on the remote gateway.

Understanding VPN policies

For each phase of negotiation, the appliance uses a policy, which is a predefined set of parameters. The appliance supports two types of security policies, Global IKE and VPN.

Global IKE Policy (Phase 1, non-configurable, except for SA lifetime parameter)

The security gateway includes a predefined global IKE policy that automatically applies to your IKE Phase 1 negotiations for all tunnels defined on the security gateway. This global IKE policy works in conjunction with the VPN policy you configure for Phase 2 negotiations. The Global IKE Policy provides the parameters that define Phase 1 negotiations of the IKE tunnel, while the VPN policy you configure and select provides the parameters for Phase 2 negotiations. There can only be one global IKE policy on a security gateway.

The only parameter in the Global IKE Policy whose setting can be changed is the SA (security association) Lifetime, which specifies the period of time after which the tunnel rekeys (in minutes). This parameter is located in VPN > Advanced > Global IKE Settings (Phase 1 Rekey). The default is 1080 minutes (18 hours). The other parameters cannot be altered.

When two security gateways are negotiating Phase 1, the first security gateway sends a list of proposals, called a transform proposal list. The security gateway to which it is connecting then selects a proposal from the list that it likes best, generally the strongest available option. You cannot change the transform proposal list on the appliance; however this information may be useful to give to the remote gateway administrator. Table 6-1 lists the order of the Symantec Gateway Security 400 IKE proposals.

Table 6-1 IKE proposal order

Data privacy	Data integrity	Diffie-Hellman
3DES	SHA1	Group 5
3DES	MD5	Group 5
3DES	SHA1	Group 2
3DES	MD5	Group 2
DES	SHA1	Group 1
DES	MD5	Group 1

Some settings are configurable at a global level for client-to-gateway tunnels. See “Configuring global policy settings for client-to-gateway VPN tunnels” on page 79.

VPN Policies (Phase 2, configurable)

The security gateway includes the following four pre-defined, configurable VPN policies that apply to Phase 2 tunnel negotiations:

- Ike_default_crypto
- Ike_default_crypto_strong
- Static_default_crypto
- Static_default_crypto_strong

Rather than configuring data privacy, data integrity, and data compression algorithms for each tunnel you create, the security gateway lets you configure standard, reusable VPN policies and then later associate them with multiple secure tunnels. You can select a pre-defined policy, or you can create your own using the VPN Policies tab.

VPN policies group together common characteristics for tunnels, and allow rapid setup of additional tunnels with the same characteristics. The security gateway also includes a handful of commonly used VPN policies for both static and dynamic tunnels.

You can define more than one VPN policy, varying the components you select for each one. If you do this, ensure that your naming conventions let you distinguish between policies that use the same encapsulation mode. When you are ready to create your secure tunnels, clearly defined naming conventions will make selecting the correct VPN policy easier.

Note: You cannot delete pre-defined VPN policies.

Creating custom Phase 2 VPN policies

VPN Policies are pre-configured for typical VPN setups. If you require customized settings (for compatibility with third-party equipment, for example), then you can create a custom Phase 2 Policy.

A VPN policy groups together common characteristics for VPN tunnels. Rather than configuring data privacy, data integrity, and data compression algorithms for each tunnel that you create, you can configure standard, reusable VPN policies, and then apply them to multiple secure tunnels.

Note: Configuring a VPN policy is optional for dynamic tunnels.

To create a custom Phase 2 VPN policy

See "VPN Policies tab field descriptions" on page 151.

1. In the SGMI, in the left pane, click **VPN**.
2. In the right pane, on the VPN Policies tab, under IPsec Security Association (Phase 2) Parameters, in the Name text box, type a name for the VPN policy.
3. To edit an existing policy, from the VPN Policy drop-down list, select a VPN policy.
4. On the Data Integrity (Authentication) drop-down list, select a type of authentication.
5. On the Data Confidentiality (Encryption) drop-down list, select an encryption type.
6. In the SA Lifetime text box, type the number of minutes you want the security association to stay alive before a rekey occurs.
   The VPN tunnel is temporarily interrupted when rekeys occur.
7. In the Data Volume Limit text box, type the number of kilobytes of traffic to allow before a rekey occurs.
8. In the Inactivity Timeout text box, type the number of minutes of inactivity before a rekey occurs.

9 To use Perfect Forward Secrecy, do the following:
- On the Perfect Forward Secrecy drop-down list, select a Diffie-Hellman group.
- Next to Perfect Forward Secrecy, click **Enable**.

10 Click **Add**.

Viewing VPN Policies List

The VPN Policies List section of the VPN Policies window displays a summary of each VPN Policy that is configured on the appliance. Table 6-2 defines each field in the VPN Policies List summary.

Table 6-2 VPN Policies List fields

Field	Description
Name	Displays the name of the VPN Policy.
Encryption Method	Displays the encryption method selected for the VPN Policy.
SA Lifetime	Displays the configured SA Lifetime setting.
Data Volume Limit	Displays the configured Data Volume Limit setting.
Inactivity Timeout	Displays the configured inactivity timeout setting.
PFS	Shows the Perfect Forward Secrecy setting.

Identifying users

The appliance lets you configure two types of VPN clients: static users and dynamic users with extended authentication.

Understanding user types

Defined users authenticate directly with the security gateway when connecting through a VPN tunnel. Static users are defined on the security gateway Client Users tab. Users with extended authentication are not defined on the security gateway; they are defined on a RADIUS authentication server. You must configure the appliance to support remote administration of users with extended authentication.

Defined users

These users authenticate using a client ID (user name) and pre-shared key that you assign to them. They enter the user name and password in their client software. That information is then sent when they attempt to create a VPN tunnel to the security gateway.

These users are defined on the appliance, and may also use extended authentication.

Users with extended authentication

Users with extended authentication are not defined on the appliance; rather, they use extended authentication with RADIUS to authenticate their tunnels. You define these users on the RADIUS server.

When a user with extended authentication attempts to authenticate, the appliance looks for that user name in the defined users list. When it does not find the user there, the appliance then uses the shared secret used by the client software. This shared secret should match the secret on the Advanced screen for the security gateway to which it is connecting. The appliance then starts extended authentication and prompts for whatever information the RADIUS server requires (such as a user name or password). The RADIUS server authenticates the user and returns the RADIUS group of the user to the security gateway. The security gateway checks that the group matches one of the client tunnels and that the group is allowed to connect to the WAN, LAN, or WLAN. If so, the user's tunnel is established.

Defining users

Ensure that you obtain all pertinent authentication information from your RADIUS administrator to pass on to your users with extended authentication.

To define users

Users must be defined on the appliance, and may also use extended authentication. Dynamic users must use extended authentication and are not defined on the appliance.

To configure users

See "Client Users tab field descriptions" on page 150.

1. In the SGMI, in the left pane, click **VPN**.
2. In the right pane, on the Client Users tab, under VPN User Identity, in the User Name text box, type the name of a new user.
3. To edit an existing user, in the User drop-down list, select a user.
4. Check **Enable**.
5. In the Pre-shared Key text box, type the pre-shared key.
6. From the VPN Group drop-down list, select a VPN group for the user to join.
7. Click **Add**.

To configure users with extended authentication

See "Advanced tab field descriptions" on page 153.

1. In the SGMI, in the left pane, click **VPN**.
2. On the Advanced tab, in the Dynamic VPN Client Settings section, do the following:
   - Check **Enable Dynamic VPN Client Tunnels**.
   - In the Pre-shared Key text box, type a key that your dynamic users will enter in their client software.
3. In the RADIUS Settings section, do the following:

Primary RADIUS Server	Type the IP address or fully qualified domain name of the RADIUS server.
Secondary RADIUS Server	Type the IP address or fully qualified domain name of the RADIUS server that the security gateway uses for authentication should the primary server become unavailable.
Authentication Port (UDP)	Type the port on the RADIUS server on which the RADIUS service runs.
Shared Secret or Key	Type the RADIUS server key.

4. Click **Save**.
5. On the Client Tunnels tab, in the VPN Group drop-down list, select the VPN group to which the users that use extended authentication belong.
6. Under Extended User Authentication, do the following:
   - Check **Enable Extended User Authentication**.
   - In the RADIUS Group Binding text box, type the name of the user's RADIUS group.
     The RADIUS group is assigned to the user on the RADIUS server. The RADIUS server must return the value that you type in the RADIUS Group Binding text box in the filterID attribute.
7. Click **Save**.

Viewing the User List

The User List section in the Client Users window displays a summary of each static user that is configured on the appliance. Table 6-3 defines each field in the summary.

Table 6-3 User list fields

Field	Description
User Name	User name entered for the static VPN user.
Enable	Indicates whether a particular user can establish VPN tunnels to the security gateway.
Pre-Shared Key	Displays the pre-shared key entered for the user.
VPN Group	Lists the VPN Groups for which a user is configured.

Configuring gateway-to-gateway tunnels

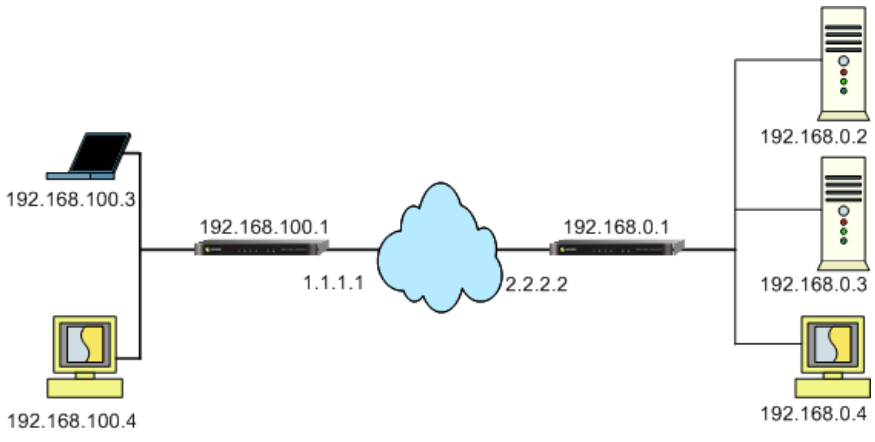
Gateway-to-gateway tunnels help secure your internal network by providing a secure bridge to an external LAN. There are several tasks involved in successfully securing the network with gateway-to-gateway tunnels. The following section describes the gateway-to-gateway tunnels, and then provides procedures for configuring the tunnels.

Understanding gateway-to-gateway tunnels

You might want to make your network resources available to an outside group, such as another office of the company. Instead of requiring each user on the second network to establish their own, private secure connection, you can create one gateway-to-gateway tunnel, which makes resources on each network available to the other. This type of tunnel is LAN-to-LAN, instead of user-to-LAN.

The appliance supports gateway-to-gateway tunnel configurations. A gateway-to-gateway configuration is created when two security gateways are connected, through an internal network, or the Internet, from WAN port to WAN port.

Figure 6-1 Gateway-to-gateway VPN tunnel configuration



This type of network configuration usually connects two subnets on the same network or, as shown in Figure 6-1, two remote offices through the Internet. Once a VPN tunnel is established, users protected by a security gateway at one site can establish a tunneled connection to the security gateway protecting the remotely located site. The remote user can connect to and access the resources of the private network as if the remote workstation was physically located inside the protected network.

The Symantec Gateway Security 400 Series can connect to another Symantec Gateway Security 400 Series appliance or to one of the following appliances:

- Symantec Gateway Security 5400 Series
- Symantec Gateway Security 300 Series
- Symantec Firewall/VPN Appliance

Symantec Gateway Security 400 Series security gateways support creating a VPN tunnel to up to five remote subnets behind Symantec Enterprise Firewall or Symantec Gateway Security 5400 Series appliances, but not to another Symantec Gateway Security 400 Series appliance or Symantec Firewall/VPN Appliance. Tunnels between two Symantec Gateway Security 400 Series appliances are only made to the subnet on the LAN side of the appliance and only support the first set (subnet/mask) of the five sets of fields, which you define on the VPN > Dynamic Tunnels or VPN > Static Tunnels tabs.

If you have another (additional) subnet on the LAN side of the Symantec Gateway Security 400 Series security gateway, VPN client tunnels to the LAN side of the security gateway are not supported for computers on this separate subnet. Only computers residing on the appliance subnet (found on the LAN IP screen) are supported for LAN/WLAN-side VPN tunnels.

You can also create global gateway-to-gateway tunnels. See "Understanding global tunnels" on page 77.

Note: Gateway-to-gateway VPN tunnels are supported on the appliance's WAN ports; you cannot define gateway-to-gateway VPN tunnels on the appliance's LAN or WLAN ports.

Supported gateway-to-gateway VPN tunnels

The Symantec Gateway Security 400 Series appliance lets you configure two types of gateway-to-gateway VPN tunnels:

Dynamic	The security gateway comes with a predefined global IKE policy that automatically applies to your IKE Phase 1 negotiations. You can change the setting of the SA Lifetime parameter in the Global IKE Policy. SA Lifetime specifies the amount of time that the tunnel rekeys (in minutes). This parameter is located in VPN > Advanced > Global IKE Settings (Phase 1 Rekey).
Static	Static gateway-to-gateway configurations require you to manually enter tunnel parameters at each security gateway. Both ends must have the same parameters, including secret keys, security parameter indexes (SPIs), authentication schemes, encryption methods.

See "Configuring gateway-to-gateway tunnels" on page 70. See "Configuring static gateway-to-gateway tunnels" on page 73.

Gateway-to-gateway VPN tunnel persistence and high-availability

After the security gateway restarts, dynamic gateway-to-gateway VPN tunnels are re-established. Dynamic gateway-to-gateway VPN tunnels are also re-established if the WAN port status changes from disconnected to connected. This feature reduces management overhead by providing automatic reconnection of tunnels.

If the VPN tunnel fails to establish after two attempts, the security gateway waits between one and five minutes before attempting to reconnect. This process continues until the VPN tunnel is re-established.

If there is a network failure, the security gateway automatically re-establishes the VPN tunnel through a backup port (WAN port or serial port). If the IP address of the security gateway changes, it re-establishes gateway-to-gateway VPN tunnels with the remote gateway using the new IP address.

Gateway-to-gateway VPN tunnel interoperability

When Symantec Gateway Security 5400 Series or Symantec Enterprise Firewall initiates a gateway-to-gateway tunnel to a Symantec Gateway Security 400 Series appliance, it begins negotiation in Main Mode.

The Symantec Gateway Security 400 Series VPN tunnel definition must be Main Mode (default), or the VPN tunnel will not be established.

While the Symantec Gateway Security 5400 Series and Symantec Enterprise Firewall accept either Main Mode or Aggressive Mode Phase 1 negotiations from a remote gateway. When initiating a VPN tunnel to Symantec Gateway Security 5400 or Symantec Enterprise Firewall, configure the Symantec Gateway Security 400 Series appliance to use Main Mode so that if the remote end initiates the VPN tunnel, it does not establish a connection.

When a non-Symantec gateway initiates a VPN tunnel to an Symantec Gateway Security 400 Series appliance, the Symantec Gateway Security 400 Series appliance accepts the mode set by the administrator on the tunnel definition.

When a Symantec Gateway Security 400 Series appliance initiates a VPN tunnel to a non-Symantec security gateway, the Symantec Gateway Security 400 Series appliance should use the mode set by the administrator on the tunnel definition; the default setting is Main Mode. If Main Mode is not used, it may cause rekey problems if the remote security gateway tries to rekey first.

Creating VPN tunnels to Symantec Gateway Security 5400 Series clusters

To create a VPN tunnel to a Symantec Gateway Security 5400 Series appliance high-availability/load balancing cluster, define the VPN tunnel using the virtual IP address of the cluster. Tunnels between Symantec Gateway 400 Series and Symantec Gateway Security 5400 Series appliances are supported in high-availability only.

Configuring dynamic gateway-to-gateway tunnels

Dynamic tunnels, also known as IKE (Internet Key Exchange) tunnels, automatically generate authentication and encryption keys. Typically, a long password, called a pre-shared key (also known as a shared secret), is entered. The target security gateway must recognize this key for authentication to succeed. If the key matches, then Security Parameter Index (SPI), authentication, and encryption keys are automatically generated and the tunnel is created. The security gateway usually re-keys (generates a new key) automatically at set intervals to ensure the continued integrity of the key.

Dynamic tunnels always use the Global IKE Policy for Phase 1 negotiation. Each tunnel uses its own VPN Policy for Phase 2. The default Phase 1 mode is Main Mode. Dynamic tunnels support up to five remote subnets or a global tunnel can be enforced. If a global tunnel is enforced, all traffic leaving the unit on the WAN port goes through the tunnel. There can be only one tunnel per WAN port which forces a global tunnel. You may configure up to 50 tunnel definitions per unit.

See “Understanding global tunnels” on page 77.

Configuration tasks for dynamic gateway-to-gateway tunnels

Table 6-4 summarizes the tasks that are required to configure dynamic gateway-to-gateway VPN tunnels.

Note: Complete each step in Table 6-4 twice: first for the local security gateway and then for the remote security gateway.

Table 6-4 Dynamic gateway-to-gateway configuration tasks

Task	Location in SGMI
Configure a VPN Policy (Phase 2 IKE negotiation) (Optional)	VPN > VPN Policies
Create a dynamic tunnel	VPN > Dynamic Tunnels

Table 6-4 Dynamic gateway-to-gateway configuration tasks (Continued)

Task	Location in SGMI
Define IPsec Security Association Parameters Select VPN Policy	VPN > Dynamic Tunnels > IPsec Security Association
Define the local security gateway	VPN > Dynamic Tunnels > Local Security Gateway
Define the remote security gateway	VPN > Dynamic Tunnels > Remote Security Gateway
Repeat the above steps for the remote security gateway.	

To configure a dynamic gateway-to-gateway tunnel

For information on creating global tunnels, see "Understanding global tunnels" on page 77.

See "Dynamic Tunnels tab field descriptions" on page 145.

1. In the left pane, click **VPN**.
2. On the Dynamic Tunnels tab, in the Name text box, type a name for the new tunnel.
   To edit an existing tunnel, from the VPN Tunnel drop-down list, select a VPN tunnel.
3. Check **Enable VPN Tunnel**.
4. On the VPN Policy drop-down list, select a VPN policy to which you want to bind to the tunnel.
5. If you have a multi-session PPPoE ISP account, under Local Security Gateway, in the PPPoE Session drop-down list, select a PPPoE session to which you want to bind to the tunnel.
   If you do not have a multi-session PPPoE ISP account, skip this step.
6. For models 460 and 460R, on the Local Endpoint drop-down list, select an endpoint for the tunnel.
7. On the ID Type drop-down list, select a Phase 1 ID type.
8. In the Phase 1 ID text box, type the Phase 1 ID.
9. Under Remote Security Gateway, do the following:
   - In the Gateway Address text box, type the remote gateway address.
   - Optionally, in the ID Type drop-down list, select a Phase 1 ID type.
   - Optionally, in the Phase 1 ID text box, type the Phase 1 ID.
   - In the Pre-Shared Key text box, type a key.
   - In each Remote Subnet IP text box, type the IP address of the destination network.
     When defining a global tunnel to Symantec Enterprise Firewall or Symantec Gateway Security 5400 Series appliance, for the remote gateway, enter 0.0.0.0 for the remote subnet IP address.
     For global tunnels to another Symantec Gateway Security 400 Series appliance, enter 0.0.0.0 for the remote subnet IP address.
   - In each Mask text box, type the netmask of the destination network.
     When defining a global tunnel to Symantec Enterprise Firewall or Symantec Gateway Security 5400 Series appliance, for the remote gateway, enter 0.0.0.0 for the netmask.
     For global tunnels to another Symantec Gateway Security 400 Series appliance, enter 255.0.0.0 for the netmask.
10. Click **Add**.

Configuring static gateway-to-gateway tunnels

Static tunnels do not use any information from the Global IKE Policy (Phase 1 negotiation). You must manually type all of the information necessary to establish the tunnel. However, you can define a VPN Policy for Phase 2 negotiation.

When defining static tunnels, you must enter an authentication key, as well as an encryption key (if encryption is used). The keys must match on both sides of the VPN. In addition, a Security Parameter Index (SPI) is manually typed and included with every packet transmitted between security gateways. The SPI is a unique gateway identifier that indicates the set of keys that belongs to each packet.

Static tunnels support up to five remote subnets or a global tunnel can be enforced. If a global tunnel is enforced, all traffic leaving the unit on the WAN port goes through the tunnel. There can be only one tunnel per WAN port which forces a global tunnel. You may configure up to 50 tunnel definitions per unit.

See "Understanding global tunnels" on page 77.

Encryption and authentication key lengths

When you define a static tunnel, you must type an encryption key and an authentication key. Each key has a specific key length based on the method that you chose. For each method, a key length is shown for both ASCII characters and Hex characters. Table 6-5 defines encryption key lengths.

Table 6-5 Encryption key lengths

Method	Key length in character bytes	Key length in Hex
DES	8	18 (0x + 16 hex digits)
3DES	24	50 (0x + 20 hex digits)
AES-128	16	18 (0x + 20 hex digits)
AES-192	24	50 (0x + 20 hex digits)
AES-256	32	66 (0x + 20 hex digits)

Table 6-6 defines authentication key lengths.

Table 6-6 Authentication key lengths

Method	Key length in character bytes	Key length in Hex
MD5	16	34 (0x + 16 hex digits)
SHA1	20	42 (0x + 20 hex digits)

Configuration tasks for static gateway-to-gateway tunnels

Table 6-7 describes the tasks that are required to configure a static gateway-to-gateway VPN tunnel.

Note: Complete each step in Table 6-7 twice; first for the local security gateway, and then for the remote security gateway.

Table 6-7 Static gateway-to-gateway configuration tasks

Task	Location in SGMI
Configure a VPN Policy (Phase 2 IKE negotiation) (Optional)	VPN > VPN Policies
Create a static tunnel	VPN > Static Tunnels
Define IPsec Security Association Parameters	VPN > Static Tunnels > IPsec Security Association
Define the remote security gateway	VPN > Static Tunnels > Remote Security Gateway
Repeat the previous steps for the remote security gateway	

To add a static gateway-to-gateway tunnel

See "Static Tunnels tab field descriptions" on page 148.

1 In the SGMI, in the left pane, click **VPN**.

2 In the right pane, on the Static Tunnels tab, under IPsec Security Association, in the Tunnel Name text box, type a name for the tunnel.
To edit an existing static tunnel, on the VPN Tunnel drop-down list, select a VPN Tunnel.

3 Check **Enable VPN Tunnel**.

4 If you have a multi-session PPPoE ISP account, under Local Security Gateway, in the PPPoE Session drop-down list, select a PPPoE session to which you want to bind to the tunnel. If you do not have a multi-session PPPoE ISP account, skip this step.

5 For models 460 and 460R, on the Local Endpoint drop-down list, select the endpoint for the tunnel.

6 In the Incoming SPI text box, type the incoming SPI to match the outgoing SPI of the remote SPI.

7 In the Outgoing SPI text box, type the outgoing SPI to match the incoming SPI on the remote side.

8 On the VPN Policy drop-down list, select a VPN policy to which you want to bind to the tunnel.
Use an existing VPN policy or create a new one.
See "Understanding VPN policies" on page 66.

9 In the Encryption Key text box, type the encryption key to match the chosen VPN policy.
Entry length must match the chosen VPN policy.

10 In the Authentication Key text box, type the authentication key to match the chosen VPN policy.

11 Under Remote Security Gateway, in the Gateway Address text box, type the gateway address to be the gateway address of the Symantec Enterprise VPN.

12 Next to NetBIOS Broadcast, click **Disable**.

13 Next to Global Tunnel, click **Disable**.

14 In the Remote Subnet IP text boxes, type the IP address of the remote subnet to the destination network.
When defining a global tunnel to Symantec Enterprise Firewall or Symantec Gateway Security 5400 Series appliance, for the remote gateway, enter 0.0.0.0 for the remote subnet IP address.
For global tunnels to another Symantec Gateway Security 400 Series appliance, enter 0.0.0.0 for the remote subnet IP address.

15 In the Mask text boxes, type the netmask of the destination network.
When defining a global tunnel to Symantec Enterprise Firewall or Symantec Gateway Security 5400 Series appliance, for the remote gateway, enter 0.0.0.0 for the netmask.
For global tunnels to another Symantec Gateway Security 400 Series appliance, enter 255.0.0.0 for the netmask.

16 Click **Add**.

Sharing information with the remote gateway administrator

Use the worksheet in Table 6-8 to list the administration information that you should provide to the administrator of the remote appliance.

Table 6-8 Configuration information to provide the remote gateway administrator

Information	Value
IP address	
Authentication key (static tunnel)	
Encryption key (static tunnel)	

Table 6-8 Configuration information to provide the remote gateway administrator (Continued)

Information	Value
SPI (Static tunnel)	
Pre-shared key	
Local subnet/mask	
VPN policy encryption method	
VPN policy authentication method	
(Optional) Local phase 1 ID	

Configuring client-to-gateway VPN tunnels

Client-to-gateway VPN tunnels let remote users running the Symantec Client VPN software (or any IPsec-compliant VPN client software) safely connect over the Internet to a network secured by a Symantec security gateway.

Understanding Client-to-Gateway VPN tunnels

Symantec Gateway Security 400 Series models 460 and 460R support client-to-gateway VPN tunnel configurations. A client-to-gateway configuration is created when a workstation, running Symantec Client VPN software, connects to the security gateway from either inside the protected network or from a remote location through the Internet. This minimizes costs associated with modem pools and costly 800 dial-up charges, as clients can use ISPs with local dial-up numbers to transparently connect to the security gateway.

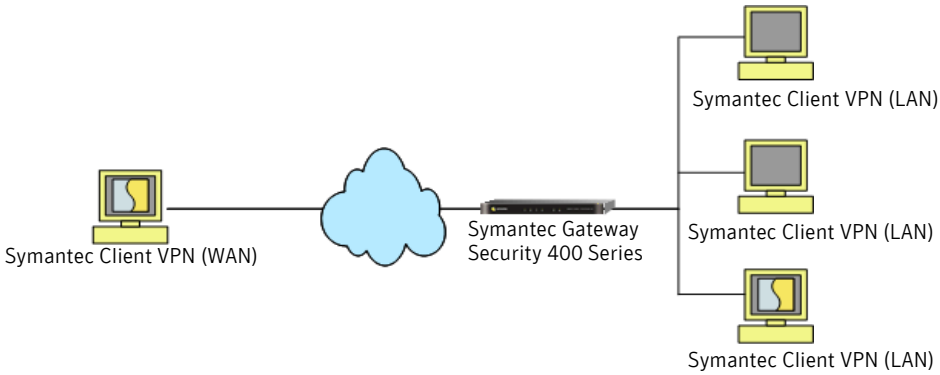
Note: Wireless clients can use client-to-gateway tunnels to secure their connections. See *Symantec Gateway Security 300/400 Series Wireless Implementation Guide*.

When Symantec Client VPN begins to negotiate a VPN tunnel with the security gateway, it does so in Aggressive mode. The security gateway will respond to this negotiation. Client-to-gateway VPN tunnels are always initiated by the client and are always in Aggressive mode.

See "Gateway-to-gateway VPN tunnel interoperability" on page 71.

Once a VPN tunnel is established, remote users can connect to and safely access the resources of the private network, through the Internet, as if the remote workstation was physically located inside the protected network (see Figure 6-2).

Figure 6-2 Client-to-gateway VPN tunnel configuration



In this diagram, a client establishes a tunnel remotely through the WAN and three internal clients establish a tunnel internally through the LAN.

For each VPN group, you can define network settings to download to the client during Phase 1 configuration mode. The settings include the primary and secondary DNS servers, the WINS servers, and the primary domain controller. By pushing this information to the clients during configuration mode, each client will not have to configure them individually, saving management time, and reducing the possibility of error.

For LAN-side VPN client tunnels, the only subnet that the client can access is the one defined on the LAN IP screen.

See "Configuring LAN IP settings" on page 49.

Symantec client-to-gateway VPN tunnels require a client ID and a shared key. You can also apply extended authentication using a RADIUS server to client-to-gateway VPN tunnels for additional authentication.

See "Defining users" on page 69.

You can configure two types of client-to-gateway users when configuring VPN tunnels: dynamic and static.

See "Identifying users" on page 68.

Understanding global tunnels

When a client establishes a VPN tunnel on the LAN, a global tunnel (0.0.0.0) is configured for the client. This forces all client traffic through the VPN tunnel terminating at the appliance. This is useful for untrusted networks, such as wireless, to keep traffic secure.

When establishing a tunnel on the WAN, the appliance's subnet (192.168.0.0 by default) is configured for the client and allows a split tunnel so that the client can still access the Internet directly and only traffic destined for the LAN is sent through the VPN tunnel.

Global tunnels terminating on the WAN port of a Symantec Gateway Security 400 Series appliance are only able to access networks on the LAN side of the appliance. When the VPN traffic arrives on the WAN port, it is decrypted and sent out on the LAN. The appliance does not support the transmission of decrypted VPN traffic on the WAN port. This means that, if a global tunnel is defined between two Symantec Gateway Security 400 Series appliances, traffic is only allowed to pass between the LAN of one appliance and the LAN of the other. No client can access the networks between the two appliances, including the Web.

Configuration tasks for client-to-gateway VPN tunnels

Table 6-9 describes the tasks that are required to configure a client-to-gateway VPN tunnel.

Table 6-9 Client-to-gateway VPN tunnel configuration tasks

Task	SGMI
Configure a VPN Policy (Phase 2 IKE negotiation) (optional)	VPN > VPN Policies
Select the VPN policy that applies to the tunnel	VPN > Advanced > Global VPN Client Settings
Identify remote users	VPN > Client Tunnels > VPN User Identity
Enable client tunnel for selected VPN Group	VPN > Client Tunnels > Group Tunnel Definition
Optionally, configure VPN network parameters (pushed to client during negotiations)	VPN > Client Tunnels > VPN Network Parameters
Optionally, configure RADIUS authentication	VPN > Client Tunnels > Extended User Authentication VPN > Advanced > RADIUS Settings
Optionally, configure Antivirus Policy Enforcement (AVpe)	VPN > Client Tunnels > Antivirus Policy

Defining client VPN tunnels

This section describes how to define client VPN tunnels.

To define client tunnels

See "Client Tunnels tab field descriptions" on page 149.

1. In the SGMI, in the left pane, click **VPN**.
2. In the right pane, on the Client Tunnels tab, under Group Tunnel Definition, in the VPN Group drop-down list, select a VPN group.
3. To enable client VPNs for the chosen VPN Group on WAN or WLAN/LAN connections, click one of the following:
   - Enable client VPNs on WAN side
   - Enable client VPNs on WLAN/LAN side
4. Optionally, under VPN Network Parameters, in the Primary DNS text box, type the name of the primary DNS server.
5. Optionally, in the Secondary DNS text box, type the name of the secondary DNS server.
   Domain Name System or Service (DNS) is an Internet service that translates domain names into IP addresses.
6. Optionally, in the Primary WINS text box, type the name of the primary WINS server.
   This is an optional step. Windows Internet Naming Service (WINS) is a system that determines the IP address associated with a particular network computer.
7. Optionally, in the Secondary WINS text box, type the name of the secondary WINS server.
8. Optionally, in the Primary Domain Controller text box, type the name of the primary domain controller.
9. Optionally, under Extended User Authentication, check **Enable Extended User Authentication**.
10. Optionally, in the RADIUS Group Binding text box, type the RADIUS Group Binding name.
    The RADIUS Group Binding name must match the filter ID parameter returned from the RADIUS server.
11. To enable Antivirus Policy Enforcement (AVpe), under WAN Client Policy, do the following:
    - Check **Enable Antivirus Policy Enforcement**.

- To log a warning to the Symantec Gateway Security log that a user is connecting that is not compliant with AVpe policy, click **Warn Only**.
- To stop the user's traffic if they are not compliant with the AVpe policy, click **Block Connections**.

12 To enable content filtering, do the following:

- Under VPN Network Parameters, in the Primary DNS text box, type the IP address or fully-qualified domain name of the security gateway.
- Under WAN Client Policy, check **Enable Content Filtering**.
- To permit traffic and block other traffic, click **Use Allow List**.
- To block traffic and permit other traffic, click **Use Deny List**.

13 Click **Update**.

Configuring global policy settings for client-to-gateway VPN tunnels

Some settings are configurable at a global level for client-to-gateway VPN tunnels. These settings configure the Phase 1 ID type for all client VPN tunnels connecting to the security gateway.

These settings are shared by all three VPN groups.

To configure global policy settings for client-to-gateway VPN tunnels

See "Advanced tab field descriptions" on page 153.

1 In the SGMI, in the left pane, click **VPN**.

2 In the right pane, on the Advanced tab, under Global VPN Client Settings, do the following:

- On the Local Gateway Phase 1 ID Type drop-down list, select an ID type.
- In the Local Gateway Phase 1 ID text box, type the value that corresponds to the ID type you selected.
- On the VPN Policy drop-down list, select a VPN policy to apply to all client tunnels.

3 Under Dynamic VPN Client Settings, do the following:

- To enable dynamic users for all three VPN groups, click **Enable Dynamic VPN Client Tunnels**.
- In the Pre-shared Key text box, type a string of characters for the key.

4 Click **Save**.

5 Click **Update**.

Sharing information with your clients

Use Table 6-10 to record information to give to your clients so that they may connect to the security gateway.

Table 6-10 Client configuration information

Information	Value
Gateway IP address or fully qualified domain name	
Pre-shared key (user)	Share this information only verbally or by other secure means.
Client ID	
RADIUS user name (Optional)	

Table 6-10 Client configuration information (Continued)

Information	Value
RADIUS shared secret (user with extended authentication) (Optional)	
Phase 1 ID (Optional)	

Monitoring VPN tunnel status

The VPN Status window lets you view the status for each configured dynamic and static gateway-to-gateway VPN tunnel. The status for static tunnels is either Enabled or Disabled; the status for dynamic tunnels is Connected, Enabled, or Disabled. The status for static tunnels is never connected because there is no negotiation for static tunnels.

The information on the Status window is current when you select it. Conditions may change while you are viewing the screen. Refresh displays the most current conditions.

To monitor VPN tunnel status

You can monitor tunnel status by verifying both ends of the tunnel, and by monitoring the Status window.

See "VPN Status tab field descriptions" on page 152.

To verify that the tunnel is operational on both ends

- From a local host, issue a PING command to a computer on the remote network.

To refresh the information on the Status window

- In the right pane, on the Status tab, on the bottom of the Status window, click **Refresh**.

Chapter 7

Advanced network traffic control

This chapter includes the following topics:

- How antivirus policy enforcement (AVpe) works
- Before you configure AVpe
- Configuring AVpe
- Monitoring antivirus status
- Verifying AVpe operation
- About content filtering
- Managing content filtering lists
- Monitoring content filtering

How antivirus policy enforcement (AVpe) works

Advanced network traffic control features of the Symantec Gateway Security 400 Series appliance include antivirus policy enforcement (AVpe) and content filtering.

AVpe lets you monitor client antivirus configurations and, if necessary, enforce security policies to restrict network access to only those clients who are protected by antivirus software with the virus definitions defined by the policy master.

The appliance also supports basic content filtering for outbound traffic. You use content filtering to restrict the URLs to which clients have access. For example, to restrict your users from seeing gambling sites, you configure content filtering to deny access to gambling URLs that you specify.

AVpe monitors the AV configuration of supported Symantec connected policy masters and client workstations attempting to gain access to your corporate network. See the *Symantec Gateway Security 400 Series Release Notes* for the version of the product you are using to determine the supported AV products and how their configuration and usage differs from the information in this chapter.

AVpe works in two different environments: a network with an internal Symantec AntiVirus Corporate Edition server that maintains antivirus information or a network of clients that are unmanaged.

If your network has an internal Symantec AntiVirus Corporate Edition server, when you configure AVpe, you designate a primary and optionally a secondary antivirus server that is accessible to your network through LAN or WAN connections. If your network has clients that are unmanaged, you designate one client as master, and all other clients verify their versions against the master.

The first time an internal client requests a DHCP connection, attempts an external connection, or any time a client initiates a VPN tunnel (originating from your LAN or remotely through the Internet), the appliance retrieves the client's antivirus policy configuration and compares it against the current antivirus policy requirements. If the client is not in compliance, the traffic is warned or blocked (as indicated when you configure AVpe) and a message is logged.

You can configure the appliance to monitor client or server configurations at specified intervals (the default setting is every 10 minutes). Once a client is connected, the appliance rechecks the client's antivirus compliance at user-defined intervals. After the specified interval (the default interval is eight hours), clients are re-queried to check for compliance. If the AV policy master shows updates were made, the clients are allowed an eight-hour grace period (the default LiveUpdate interval on unmanaged clients) in which they will still be compliant if they have the last AV policy master definition version. After this grace period, the clients will be considered non-compliant with the AV policy.

Table 7-1 describes client compliance and the subsequent actions taken.

Table 7-1 Client compliance actions

Client status	Action
Compliant with current antivirus policies	Client is granted access to the firewall.
Antivirus protection is out-of-date	The connection is allowed to pass, but the appliance logs a warning or completely blocks access, depending on the option you select.

Clients who have been denied access can still connect to Symantec AntiVirus Corporate Edition or Symantec LiveUpdate servers to update their virus definitions.

You determine whether to enforce antivirus compliance for local clients using computer groups or VPN groups. All local clients belong to computer groups. For each computer group, you enable or disable AVpe. The default AVpe status for all computer groups is disabled.

See "Understanding computers and computer groups" on page 53.

Similarly, all VPN users are members of VPN groups. For each VPN group, you can enable or disable AVpe on the Client Tunnels tab in the SGMI. The default AVpe status for all VPN groups is disabled.

See "Defining client VPN tunnels" on page 78.

If content filtering and antivirus policy enforcement are enabled at the same time, content filtering takes precedence over antivirus policy enforcement processing for outbound traffic only. If a content filtering violation occurs and a client is blocked from viewing content, a message is logged and no antivirus policy enforcement rules are processed.

AVpe is supported for outbound connections and VPN client connections (LAN or WAN) only.

Before you configure AVpe

Before configuring the AVpe feature, do the following:

- Include your AVpe needs in your strategy for group assignments. AVpe is supported for outbound connections and VPN client connections only. Determine those clients whose virus definitions will be checked and those (if any) who will be allowed conditional or unconditional network access. Then assign users to the appropriate access or VPN groups and select whether you will warn or block non-compliant clients who attempt to access the local network.
  See "Defining computer groups" on page 55 or "Viewing the User List" on page 70.

  Note: You must place UNIX/Linux clients or clients with a non-supported AV client in a computer group where AVpe is disabled.

- If you plan to use Symantec AntiVirus Corporate Edition servers, obtain the name of the primary and optionally the secondary servers used in your network.
- If your network is comprised of clients that are unmanaged and access LiveUpdate directly for their AV updates, decide which client to designate as the master. The master should always be turned on, have

an active Symantec antivirus client, and have a connection to the Internet where it can download virus definition updates.

- If your network topology includes a configuration in which client workstations are located behind an enclave firewall, and if the firewall performs address transforms, which changes the client's actual IP address, the security gateway is unable to communicate with the client (as is required to validate client virus definitions). In this configuration, the security gateway contacts the firewall, not the client.
- Ensure that traffic is not being blocked by a personal firewall. You must allow UDP/Port 2967 on all personal firewalls. This is set by default in Symantec Client VPN version 8.0.

Configuring AVpe

Configuring AVpe for a Symantec AntiVirus Corporate Edition environment and a client-only network is similar.

Configuring for Symantec AntiVirus Corporate Edition servers involves the following tasks:

- Defining the location of the primary and (optionally) a secondary Symantec AntiVirus server and verifying that a client has the Symantec AntiVirus Corporate Edition client installed and that the virus definitions and the scanning engine on client computers are up-to-date.
  See "Configuring AVpe" on page 83.
- Enabling AVpe for Computer or VPN Groups.
  See "Enabling AVpe" on page 84.

Configuring for networks with unmanaged antivirus clients (without Symantec AntiVirus Corporate Edition) involves the following tasks:

- Defining the location of the policy master client and verifying that it has a supported Symantec antivirus client installed and that the virus definitions and the scanning engine on client computers are up-to-date.
- Enabling AVpe for Computer or VPN Groups.
  See "Enabling AVpe" on page 84.
- Configuring the AV clients.
  See "Configuring the antivirus clients" on page 85.

To configure antivirus policy enforcement

See "Antivirus Policy field descriptions" on page 156.

1. In the SGMI, in the left pane, click **Antivirus Policy**.
2. In the Primary AV Master text box, in the right pane, under Server Location, type the IP address or fully qualified domain name of your primary antivirus server or master client.
3. Optionally, in the Secondary AV Master text box, type the IP address or fully qualified domain name of a backup antivirus server, if supported in your environment.
4. In the Query AV Master Every text box, type an interval (in minutes) for the appliance to query the antivirus server for updated virus definitions.
5. To force a manual update, click **Query Master**.
6. Under Policy Validation, next to Verify AV Client is Active, select one of the following:
   - Latest Product Engine
     To check a client's antivirus configuration to ensure it uses a supported Symantec antivirus product with the latest product scan engine.
   - Any Version
     To check a client's antivirus configuration to verify that the correct version of a supported Symantec antivirus product is installed on the client's workstation.

7 To enable the appliance to validate whether a client is using the latest virus definitions, check **Verify Latest Virus Definitions**.

8 In the Query Clients Every text box, type an interval (in minutes) for the appliance to query clients to validate whether they are using updated virus definitions.

9 Click **Save**.

Enabling AVpe

AVpe is enforced at the computer group and VPN group level. To enable AVpe, you first select a group, and then enable AVpe once for all members of that group. You also decide whether you want to warn or to deny WAN access to clients if their antivirus configuration is not compliant with expected security policies.

To enable AVpe

After you have configured AVpe, you must enable it for each computer group or VPN group.

Enabling AVpe for VPN groups is for WAN clients only. You enable AVpe for LAN VPN clients on the Client Tunnels tab in the VPN section. You enable AVpe for computer groups on the Computer Groups tab in the Firewall section.

See "Defining computer groups" on page 55.

See "Defining client VPN tunnels" on page 78.

See "Computer Groups tab field descriptions" on page 138.

See "Client Tunnels tab field descriptions" on page 149.

To enable antivirus policy enforcement for computer groups

1 In the SGMI, in the left pane, click **Firewall**.

2 On the Computer Groups tab, under Security Policy, on the Computer Group drop-down list, select the computer group for which you want to enable AVpe.

3 Under Antivirus Policy Enforcement, check **Enable Antivirus Policy Enforcement**, and then do one of the following:

- To log warnings for clients with out-of-date virus definitions, click **Warn Only**.
- To completely block connections from clients with out-of-date virus definitions, click **Block Connections**.

4 Click **Save**.

5 Repeat steps 2 through 4 to enable AVpe for each computer group.

To enable antivirus policy enforcement for VPN groups

1 In the SGMI, in the left pane, click **VPN**.

2 In the right pane, on the Client Tunnels tab, under Group Tunnel Definition, on the VPN Group drop-down list, select the VPN group for which you want to enable AVpe.

3 Under WAN Client Policy, check **Enable Antivirus Policy Enforcement**, and then do one of the following:

- To log warnings for clients with out-of-date virus definitions, click **Warn Only**.
- To completely block connections from clients with out-of-date virus definitions, click **Block Connections**.

4 Click **Save**.

5 Repeat steps 2 through 4 to enable AVpe for each desired VPN group.

Configuring the antivirus clients

If the clients on your network are unmanaged and use LiveUpdate to install current virus definitions and engines, you must configure each client before it can be validated using AVpe. Each client that you want to validate with AVpe must have a supported Symantec antivirus product installed in unmanaged mode.

When you uninstall the client software, the registry keys that are created by this procedure are also removed.

Warning: Do not use this procedure for clients managed by a Symantec AntiVirus server.

To configure the AV clients

1. Install or configure each client's supported Symantec antivirus product in unmanaged mode.
2. Insert the Symantec Gateway Security 400 Series product CD into the CD-ROM drive on a client computer.
3. In the Tools folder on the CD-ROM, copy SGS300_AVpe_client_Activation.reg to the client's desktop.
4. Double-click the file.
5. Repeat steps 2-4 for each client that you want to be validated using AVpe.

Monitoring antivirus status

The AV Master Status and AV Client Status sections of the AVpe tab lets you obtain an operational status of the primary and secondary antivirus master and clients configured in your network.

Any changes you make to the configuration of the primary or secondary antivirus server, once saved, are reflected in the AV Master Status field.

Viewing AVpe log messages

When you enable AVpe and a client connection is denied (either because it is blocked or warned), a message is logged. You can view these log messages periodically to monitor your traffic.

To view AVpe log messages

See "View Log tab field descriptions" on page 119.

1. In the SGMI, in the left pane, click **Logging/Monitoring**.
2. On the View Log tab, click **Refresh**.

Verifying AVpe operation

After you have enabled AVpe, you can test its operation by disabling Symantec AntiVirus Corporate Edition on a client workstation and then attempting to connect to the local network. If antivirus policy enforcement is properly configured, in the absence of enabled Symantec antivirus software, all connection attempts should be blocked or warned.

The status of the secondary antivirus server is not displayed unless the primary server is unreachable.

Note: The client workstation does not receive any notification that network access is blocked and a message is logged.

To verify antivirus policy enforcement operation

See "Logging/Monitoring field descriptions" on page 117.

1. Uninstall Symantec AntiVirus Corporate Edition from a client workstation that has been configured as part of a computer group with AVpe enabled, with connections blocked.
2. Open a Web browser and attempt to connect to www.symantec.com.
   The connection attempt should fail and all communication through the firewall should be blocked.
3. In the SGMI, in the left pane, click **Logging/Monitoring**.
4. Click **View Log** and check for a warning message indicating that all connection attempts for the particular client are blocked due to policy non-compliance.
   If this message is present, then your AVpe feature is correctly configured and operational.
5. If you are able to connect to www.symantec.com, recheck your AVpe configuration settings and group assignments. Make sure that you uninstalled Symantec AntiVirus Corporate Edition from the client workstation, and that the client is a member of a group with AVpe enabled, with connections blocked. Retry steps 1 through 4 above.

About content filtering

Symantec Gateway Security 400 Series supports basic content filtering for outbound traffic. You use content filtering to restrict the content to which clients have access. For example, to restrict your users from seeing gambling sites, you configure content filtering to deny access to gambling URLs that you specify.

Content filtering is administered through computer groups and VPN groups. A computer group is a group of computers defined in the Firewall section to which you apply the same rules. Similarly, a VPN group is a group of VPN users defined in the VPN section to which you apply the same rules. When you define a computer group or VPN group, you specify if the group uses a content filtering deny or allow list. Deny lists (black lists) block internal access to sites on the list and allows all others sites. Allow lists (white lists) permit internal access to sites on the list, and blocks access to all other sites.

Note: By default, content filtering is disabled for all computer groups and VPN groups.

The allow list permits traffic to pass to sites that exactly match entries in the list. The content filtering engine drops connection requests sent to a destination that do not match the entries in the list. If the allow list is empty, all traffic is blocked.

If the deny list is empty, traffic is not filtered. Once entries are added to the deny list, the content filtering engine drops connection requests sent to a destination that exactly matches an entry. Traffic that does not match an entry is allowed to pass.

Special considerations

When content filtering and AVpe are concurrently enabled, content filtering is performed first. If the content filtering results in a blocked connection, AVpe is not processed; only a content filtering message is logged.

If you make changes to content filtering on the appliance, clear the DNS and browser caches on the client machine. If a URL is accessed by a client, but then the content filtering settings change to deny access to that URL, the cache may be used and allow the client access to the URL. Refer to your operating system documentation for information on clearing DNS caches and your browser's documentation for clearing the browser cache.

If you enable content filtering for remote WAN-side VPN clients, you must have DNS servers on the local LAN.

If a site or security gateway uses redirection to transfer users from one URL to another, you must include both URLs in the list. For example, www.disney.com redirects users to www.disney.go.com. To let your users view this Web site, you must specify both www.disney.com and www.disney.go.com in the allow list.

If a site brings in content from other sites, you must add both URLs to the list. For example, www.cnn.com uses content from www.cnn.net.

Managing content filtering lists

When you create allow and deny lists, you provide the allowed or denied fully qualified domain names. The appliance filters traffic by checking DNS lookup requests. There must be an exact match on the destination for action (blocking or warning) to occur.

For wild card functionality, specify only the domain name in the allow or deny list for specific sites. For example, to allow traffic to any Symantec site, add symantec.com to the allow list. This allows traffic to liveupdate.symantec.com, www.symantec.com, fileshare.symantec.com, and so on.

Content filtering applies to all outbound traffic, not just HTTP (Web) traffic.

To manage allow and deny lists

By default, the allow and deny lists are empty. Each filtering list can hold up to 100 entries. Each entry can be up to 128 characters long.

See "Content Filtering field descriptions" on page 157.

To add a URL to an allow or deny list

1. In the SGMI, in the left pane, click **Content Filtering**.
2. Under Select List, next to List Type, select **Allow** or **Deny**.
3. In the Input URL text box, type the name of a site that you want to add to the list. For example, yoursite.com.
4. Click **Add**.
   Repeat steps 3 and 4 until you have added all URLs to the list.
5. Click **Save List**.

To remove a URL from an allow or deny list

1. In the SGMI, in the left pane, click **Content Filtering**.
2. From the Delete URL drop-down list, select the URL that you want to delete.
3. Click **Delete Entry**.
4. Click **Save List**.

Enabling content filtering

Content filtering is enforced at the computer group and VPN group level. After you have set up the allow or deny lists, you must enable content filtering for each computer group or VPN group for which you want to filter traffic. See "Defining inbound access" on page 56.

To enable content filtering

You can enable content filtering for LAN-based clients using the Computer Groups tab in the Firewall section. You can enable content filtering for WAN-based clients using the Client Tunnels tab in the VPN section.

To enable content filtering for a computer group

See "Computer Groups tab field descriptions" on page 138.

1 In the left pane, click **Firewall**.

2 On the Computer Groups tab, under Security Policy, in the Computer Group drop-down list, select the computer group for which you want to enable content filtering.

3 Under Content Filtering, check **Enable Content Filtering** and do one of the following:

- To filter content based on the deny list, click **Use Deny List**.
- To filter content based on the allow list, click **Use Allow List**.

4 Click **Save**.

To enable content filtering for a VPN group

See "Client Tunnels tab field descriptions" on page 149.

1 In the left pane, click **VPN**.

2 On the Client tunnels tab, under Group Tunnel Definition, in the VPN Group drop-down list, select the VPN group for which you want to enable content filtering.

3 Under WAN Client Policy, check **Enable Content Filtering** and do one of the following:

- To filter content based on the deny list, click **Use Deny List**.
- To filter content based on the allow list, click **Use Allow List**.

4 Click **Save**.

Monitoring content filtering

Content filtering logs a message in the log files if packets are dropped due to a user attempting to access a URL on the deny list, or attempting to access a URL that is not specifically permitted on the allow list.
See "Logging, monitoring and updates" on page 93.

You can view the URLs and their status that are on either the allow or deny list.

To view a list of URLs on the allow or deny list

See "Content Filtering field descriptions" on page 157.

1 In the left pane, click **Content Filtering**.

2 Under Select List, under List Type, do one of the following:

- To view the URLs on the Deny list, click **Deny**.
- To view the URLs on the Allow list, click **Allow**.

3 Click **View/Edit**.

Chapter 8

Preventing attacks

This chapter includes the following topics:

- Intrusion detection and intrusion prevention
- Setting protection preferences
- Enabling advanced protection settings

Intrusion detection and intrusion prevention

The Symantec Gateway Security 400 Series intrusion detection and intrusion prevention (IDS and IPS) feature helps secure your network against unwanted intruders and attacks. IDS/IPS monitors the network for suspicious behavior, and lets you respond to detected intrusions in real-time.

IDS/IPS functionality is enabled by default, but you can disable it using the Security Gateway Management Interface (SGMI). IDS/IPS logging is also enabled by default. Any event logged by the IDS engine is identified as such in log messages. If you disable IDS and IPS logging, the security gateway still blocks any connection attempt to an unauthorized service for inbound connections, but the Trojan horse lookup is disabled and log messages are limited to an access denied message.

The number of log messages that are tracked depends on the attack type. There is no limit to the number of logged management login attempts. Attack logging is limited to one message in five seconds; if more than one occurrence of the same attack is discovered within a five second window, only one message is generated. When ICMP blocking is enabled, the log messages are not limited.

Atomic packet inspection

The IDS engine provides atomic packet inspection by comparing each inbound packet against a list of signatures (known attacks). Matching packets are considered intrusion attempts and dropped.

The Symantec Gateway Security 400 Series has signatures for, and can detect, the following types of intrusions:

- Bonk
- Fawx
- Jolt
- Land
- Nestea
- Newtear
- Overdrop
- Ping of Death
- Syndrop

- Teardrop
- Winnuke
- HTML buffer overflow
- TCP/UDP flood protection

Trojan horse notification

Any attempt to connect to a blocked port that is commonly used by Trojan horse programs is logged and classified as a possible attack. The log message warns the user that an illegal connection attempt was made and that they should audit their internal systems to verify they are not compromised. Trojan horse protection is overridden if traffic is explicitly allowed in an inbound rule.

Connections to the ports listed in Table 8-1 generate warnings in the log file, unless you specifically have a rule configured to allow inbound traffic on that port.

Table 8-1 Trojan horse ports and protocols

Trojan horse	Protocol	Ports
Back Orifice	TCP	31337
	UDP	31337
Girlfriend	TCP	21554
Portal of Doom	TCP	3700, 9872, 9873, 9874, 9875, 10067, 10167
	UDP	10067, 10167
SubSeven	TCP	1243, 6711, 6712, 6713, 6766, 27374, 27573
	UDP	27573

Setting protection preferences

For each atomic IDS and IPS signature, you can set the action to take with detection of each individual signature, as follows:

- Block and Warn
  Drop and log packets identified as containing the specific signature.
- Block/Don't Warn
  Drop the packet; but do not log.

You can configure the following options for enabling and disabling IDS and IPS signature detection and logging:

- Select All to enable or disable detection of ALL signatures.
- Enable/disable detection of each signature individually.

To set protection preferences

See "IDS Protection tab field descriptions" on page 154.

1. In the SGMI, in the left pane, click **IDS/IPS**.
2. In the right pane, on the IDS Protection tab, under IDS Signatures, from the Name drop-down list, select an IDS signature.
   To apply the preferences to all the signatures, click **>>Select All<<**.
3. Under Protection settings, next to Action, select an action.

4 Next to Protection Area, select an interface to protect.

5 Click **Update**.

Enabling advanced protection settings

Advanced protection settings help you protect your network beyond attacks that can be identified by atomic signatures.

IP spoofing protection

Any non-broadcast or multicast packet arriving on a WAN interface with a source IP address that matches any internal subnet is blocked and flagged as an IP spoofing attempt. Internal subnets are derived from the LAN side subnet address of the appliance and the static route entries on the appliance for the LAN interface.

Likewise, any non-broadcast or non-multicast traffic that arrives at the internal or wireless interface with a source IP address that does not match any predefined internal network is blocked and logged as an internal IP spoofing attempt. Internal networks are derived from static routes on the unit and the internal LAN/WLAN address of the unit. Spoof protection can be disabled for the internal LANs and WAN.

To enable IP spoof protection

See "IDS Protection tab field descriptions" on page 154.

1 In the SGMI, in the left pane, click **IDS/IPS**.

2 In the right pane, on the Advanced tab, under IP Spoof Protection, check **WAN** or **WLAN/LAN**.

3 Click **Save**.

TCP flag validation

Certain port mapping tools, such as NMAP, use invalid TCP flag combinations to detect a firewall on a network or map the security policy implemented on the firewall. Symantec Gateway Security 400 Series blocks and logs any traffic with illegal flag combinations for traffic that is not being denied by the security policy. Any traffic denied by the security policy that has one or more bad TCP flag combinations is classified as one of several NMAP port scanning techniques (NMAP Null Scan, NMAP Christmas Scan, and so on).

To enable TCP flag validation

See "IDS Protection tab field descriptions" on page 154.

1 In the SGMI, in the left pane, click **IDS/IPS**.

2 In the right pane, on the Advanced tab, under TCP Flag Validation, check **Enable**.

Chapter 9

Logging, monitoring and updates

This chapter includes the following topics:

- Managing logging
- Updating firmware
- Backing up and restoring configurations
- Interpreting LEDs
- LiveUpdate and firmware upgrade LED sequences

Managing logging

The firewall, IDS, IPS, VPN, content filtering, and AVpe features log messages when certain events occur. You can configure the events that are logged so you view only the log messages of interest.

You can view the log messages through the SGMI, or forward them to external services. Log messages are maintained until the appliance is restarted. On all appliances, the 100 most current messages are available to view and are maintained, even if the appliance is restarted.

When the log is full, new entries overwrite the oldest ones. You should set up either email forwarding or a Syslog server if you want to retain old log messages. See "Emailing log messages" on page 93 or "Using Syslog" on page 94.

Configuring log preferences

Logging preferences let you set the way in which log messages are viewed, the amount of logging that is performed, and how to log files are handled when the log becomes full. The following settings help you create logging scenarios that are appropriate to your network's needs:

- Emailing log messages
- Using Syslog
- Configuring and verifying SNMP
- Selecting logging levels
- Setting log times

Emailing log messages

You can configure the appliance to automatically email log entries when the log is full or if an attack is detected. The log file is sent as a text message.

To configure email forwarding

See "Log Settings tab field descriptions" on page 120.

1. In the SGMI, in the left pane, click **Logging/Monitoring**.
2. On the right pane, on the Log Settings tab, in the SMTP Server text box, type the IP address or DNS name of the Simple Mail Transfer Protocol (SMTP) server that you want to receive the Log file.
3. In the Send Email From text box, type the email address of the sender of the email.
4. In the Send Email To text box, type the email address of the receiver of the email.
5. Click **Save**.
6. To send the current log messages without waiting for the log to become full, click **Email Log Now**.

Using Syslog

Sending log messages to a Syslog server lets you store log messages for long term. A Syslog server listens for log entries forwarded by the appliance and stores all log information for future analysis. The Syslog server can be on the LAN or WAN, or behind a VPN tunnel.

Note: The date and time on messages in the Syslog server are the time they arrived at the Syslog server, and not the time that the appliance logged the event that triggered the log message.

To use Syslog

See "Log Settings tab field descriptions" on page 120.

1. In the SGMI, in the left pane, click **Logging/Monitoring**.
2. In the right pane, on the Log Settings tab, under Syslog, in the Syslog Server text box, type the IP address of a host running a standard Syslog utility to receive the log file.
3. Click **Save**.

Configuring and verifying SNMP

The appliance supports Simple Network Management Protocol (SNMP) version 1.0 and generates network event alert messages, copies them into an SNMP TRAP or GET with the associated community name, and then sends them to registered SNMP servers. This capability lets the appliance report status information to network-wide SNMP-based management applications. The appliance generates SNMP messages for the following events:

- Start-up of the appliance
- SGMI authentication failure
- Ethernet WAN ports up and down
  - No trap when WAN ports comes alive as part of system startup
  - WAN disconnect
  - WAN coming back after a previous disconnect
- Serial WAN port (PPPoE or Analog)
  - WAN Link up (connected)
  - WAN Link down (disconnected)

A GET is a request from the SNMP server for status information from the Symantec Gateway Security 400 Series appliance. The appliance supports all SNMP v1 MIBS (information variables) using GETs. A TRAP collects status information set from Symantec Gateway Security 400 Series appliance to the SNMP server.

Configuring SNMP sets the IP addresses of the SNMP servers to receive status information (TRAPS) alerts from the SNMP agent running on the appliance. This feature provides minimal protection over a public

network; therefore, for highest security, remote access administration should be done through a VPN tunnel.

To monitor the appliance on the LAN side, browse to the appliance's LAN IP address (by default, 192.168.0.1) using an SNMP v1 MIB browser. To allow external access to SNMP GET on the appliance, check Enable Remote Monitoring on the Administration > SNMP tab in the SGMI.

Configuring SNMP

There are two parts to configuring SNMP:

- Configuring SNMP
- Verifying communication between the SNMP server and the Symantec Gateway Security 400 Series appliance.

Before you begin configuring SNMP, collect the following information:

- For TRAPs, you must have SNMP v 1.0 servers or applications running on your network to receive the network event alert messages and you need the SNMP server IP addresses to configure SNMP on the appliance.
- You also need the community string for the SNMP server. The SNMP server IP address and community string should be available from the administrator running the SNMP server.
- You can configure SNMP at anytime after the appliance is installed and the SNMP servers are running.

See "Administration field descriptions" on page 121.

To configure SNMP

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the SNMP tab, under SNMP Read-only Managers (GETS and TRAPS), in the Community String text box, type the name of the community.
   The default is Public.
3. In the IP Address text boxes, type the IP addresses of the SNMP read-only managers (for TRAP collection only).
4. Click **Save**.

To verify SNMP communication

- Contact the SNMP server administrator and have them send a GET from the SNMP server to your appliance.

The appliance responds by sending status information to the SNMP server.

If it does not respond, check that the SNMP server IP address and community string are correct. Also check that the SNMP server is accessible from the appliance.

Selecting logging levels

The log file contains only the types of information you choose. This is useful for isolating a problem or attack.

If you select Debug information, performance may be affected by the number of messages that are created. You should select this option only for troubleshooting purposes, and then disable it when you are done.

To select log levels

See "Logging/Monitoring field descriptions" on page 117.

1. In the SGMI, in the left pane, click **Logging/Monitoring**.

2 In the right pane, on the Log Settings tab, under Log Type, check the types of information you want to be logged.

3 Click **Save**.

Setting log times

Network Time Protocol (NTP) is an Internet standard protocol that ensures accurate synchronization, to the millisecond, of computer clock times in a network.

If you do not configure an NTP server, standard public NTP servers are used. If an NTP server is not reachable, when an event occurs, the appliance records the time (in seconds) since the last reboot.

To set log times

See "Log Settings tab field descriptions" on page 120.

1 In the SGMI, in the left pane, click **Logging/Monitoring**.

2 In the right pane, on the Log Settings tab, under Time, in the NTP Server text box, type the IP address or fully qualified domain name of the non-public NTP Server.

3 Click **Save**.

Managing log messages

The View Log tab shows the current conditions of the appliance. Models 460 and 460R have a WAN 2 section for the second WAN port status.

The information on the View Log tab is current when you click it. Conditions may change while you are viewing the screen. Refresh updates the View Log tab to display the most current messages.

You can manually delete the contents of the log at any time.

To manage log messages

After log messages have been generated, you can view them, refresh them to see the most current messages, or clear the log if you no longer want those messages.

See "View Log tab field descriptions" on page 119.

To view log messages

1 In the SGMI, in the left pane, click **Logging/Monitoring**.

2 Do one of the following:

- On the View Log tab, view the log messages.
- To view older log messages, click **Next Page**.

To refresh log messages

1 In the SGMI, in the left pane, click **Logging/Monitoring**.

2 In the right pane, on the View Log tab, click **Refresh**.

To clear log messages

1 In the SGMI, in the left pane, click **Logging/Monitoring**.

2 In the right pane, on the View Log tab, click **Clear Log**.

Updating firmware

The appliance runs using a set of instructions that are coded into its permanent memory called firmware. The firmware contains all of the features and functionality of the appliance. There are two types of firmware updates: destructive and non-destructive. Destructive firmware updates completely overwrite the firmware and all of the configuration settings. Non-destructive firmware updates overwrite the firmware but keep the configurations intact.

Symantec periodically releases updates to the firmware. There are three ways to update the firmware on your appliance:

- Automatically using the Scheduler in LiveUpdate
- Manually using LiveUpdate
- Manually by receiving firmware from Symantec Technical Support and applying it using the symcftpw tool.

By default, LiveUpdate checks for updates at the end of the Setup Wizard. You may disable this feature. See the *Symantec Gateway Security 400 Series Installation Guide*.

Warning: Performing a manual firmware upgrade with app.bin may overwrite your configuration settings. Before performing an upgrade, make note of your settings. Do not use a configuration backup file of older firmware on newer firmware. LiveUpdate firmware upgrades never overwrite your configuration.

When you apply a firmware upgrade manually or through LiveUpdate, the LEDs flash in a unique sequence that indicates the progress.

See "LiveUpdate and firmware upgrade LED sequences" on page 106.

Automatically updating firmware

LiveUpdate is a Symantec technology that enables you to automatically keep your Symantec products up-to-date with the latest revision. You can configure LiveUpdate to check for updates automatically, or you can manually run LiveUpdate at any time to check for updates.

Symantec periodically releases firmware updates to ensure the highest level of security available. Run LiveUpdate as soon as your Symantec Gateway Security 400 Series appliance is connected to the Internet.

See "Running LiveUpdate Now" on page 101.

When LiveUpdate checks for firmware updates, if a new firmware package is found, LiveUpdate downloads and begins applying the firmware without prompting the administrator. During the download and application, the SGMI displays a message stating that an update is being applied and to wait a few minutes before attempting to log into the SGMI. Afterwards, the appliance may restart. When firmware application is complete, a message is logged.

If LiveUpdate checks for firmware updates and none are available (the current firmware is up-to-date), a message is logged.

All LiveUpdate packages posted by Symantec are tested and validated by Symantec. These packages do not intentionally overwrite your current configuration. However, they require an automatic restart of the appliance. To minimize downtime or interruption to your network connectivity, use the Preferred Time feature to schedule updates during off hours.

The LiveUpdate functionality provides a fail-safe mechanism for firmware updates if the appliance becomes non-usable (such as a power outage during the LiveUpdate upload). If the appliance is unable to pass its self-check test with a new LiveUpdate package, it reverts to the factory firmware stored in protected memory. LiveUpdate only downloads and applies non-destructive firmware.

Scheduling automatic updates

LiveUpdate runs in automatic or manual mode. In automatic mode, the appliance checks for new updates. If you schedule automatic updates, each time the appliance is restarted, LiveUpdate checks for updates. Also, if you change the appliance from manual updates to automatic, LiveUpdate checks for updates at the next time you specify in the UTC text box.

If LiveUpdate downloads and applies a new firmware update, the appliance may restart. For this reason, you should schedule automatic updates to occur during your network's down time.

To schedule LiveUpdate for automatic updates

See "Trusted Certificates tab field descriptions" on page 123.

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the LiveUpdate tab, under Automatic Updates, check **Enable Scheduler**.
3. From the Frequency drop-down list, select the frequency with which the appliance checks for updates.
4. In the Preferred Time (UTC) text box, type the time of day, in hours and minutes, that you want the appliance to check for updates; for example 20:00 for 8:00 PM.
5. Click **Save**.

Allowing automatic updates through an HTTP proxy server

LiveUpdate optional settings let you configure a connection to a LiveUpdate server through an HTTP proxy server. Use this feature only in the following situations:

- The appliance is located behind a Symantec Gateway Security appliance using an HTTP proxy server.
- The appliance is located behind a third party device using HTTP proxy server.
- Your ISP uses an HTTP proxy server.

For more information, refer to Symantec LiveUpdate documentation.

See "Trusted Certificates tab field descriptions" on page 123.

To allow automatic updates through an HTTP proxy server

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the LiveUpdate tab, under Optional Settings, check **HTTP proxy Server.**
3. In the Proxy Server Address text box, type the IP address or fully qualified domain name of the HTTP proxy server.
4. In the Port text box, type the port number.
5. In the User Name text box, type the proxy user name.
6. In the Password text box, type the proxy password.
7. Click **Save**.

Changing the LiveUpdate server location

By default, the LiveUpdate settings point to liveupdate.symantec.com. You can also configure the appliance to use your own LiveUpdate staging server instead of the Symantec LiveUpdate site.

The internal LiveUpdate servers shown in Figure 9-1 are configured using the Symantec LiveUpdate Administration Utility. Rather than the appliance contacting the Symantec servers to obtain product updates, the appliance can contact the LiveUpdate server on the local network. This greatly reduces network traffic and increases transfer speeds. It also lets you stage, manage, and validate updates before applying them. The LiveUpdate Administration Utility and instructions for installation are available on the Symantec Technical Support Web page http://www.symantec.com/techsupp/.

Table 9-1 shows and lists the LiveUpdate server configurations shown in Figure 9-1.

Figure 9-1 LiveUpdate configurations.

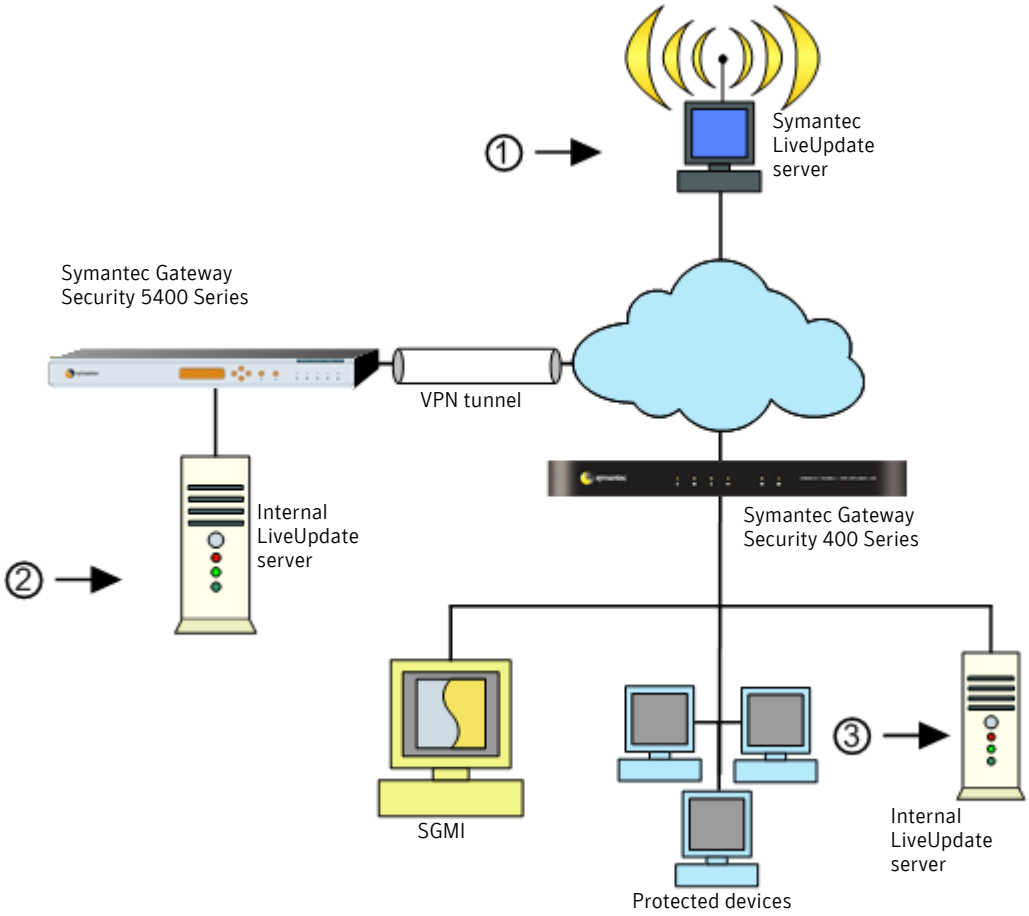


Table 9-1 LiveUpdate server configurations

Location	Description
1	Symantec LiveUpdate server: http://liveupdate.symantec.com. This is the standard Symantec corporate LiveUpdate site which broadcasts firmware availability. It is the default configuration in your appliance.
2	Internal Live Update server at a remote internal location, protected by a VPN tunnel.
3	Internal LiveUpdate server at a local location.

LiveUpdate servers can be on the WAN or LAN, or accessible through a Gateway-to-Gateway VPN tunnel.

See "Trusted Certificates tab field descriptions" on page 123.

To change the LiveUpdate server location

1 In the SGMI, in the left pane, click **Administration**.

2 In the right pane, on the LiveUpdate tab, under General Settings, in the LiveUpdate Server text box, type the IP address or fully qualified domain name for your LiveUpdate server.

3 Click **Save**.

Upgrading firmware manually

Firmware upgrades are available from Symantec's Web site. If you do not configure LiveUpdate to automatically download and apply firmware upgrades; or if you are instructed to manually perform an upgrade by Symantec Technical Support, you should check the Symantec Web for the latest version of the firmware. Your current firmware version number is available on the Status tab.

The firmware file that is available from Symantec Technical Support is called all.bin. It overwrites your configuration, so before you begin a manual firmware upgrade, make note of your configuration. The only setting that it leaves intact is the administrator's password.

See "Setting the administration password" on page 18.

Warning: Re-flashing the firmware with an old version of the firmware erases all previous configuration information including the password.

Apply the firmware by using the Symantec FTP utility (included on the Symantec Gateway Security 400 Series CD-ROM), or you can use the DOS TFTP command with the -i (binary) option. This transfers the firmware file to the appliance, applies it, and then restarts the appliance.

Flashing the firmware

Before you perform a manual firmware upgrade, ensure you have the following items:

- symcftpw utility
  Located on the Tools folder on the CD-ROM included with your appliance. You may also use the TFTP command to put firmware on the appliance.
- Firmware file
  Download the latest firmware file from Symantec's Web site.

Note: If the computer on which you run symcftpw has Norton Internet Security installed, you must configure both an inbound rule and an outbound rule in Norton Internet Security to permit the traffic between the computer and the appliance.

Figure 9-2 shows the rear panel on models 420 and 440. This figure is for reference only; the full description of each feature is available in the *Symantec Gateway Security 400 Series Installation Guide*.

Figure 9-2 Models 420 and 440 rear panel

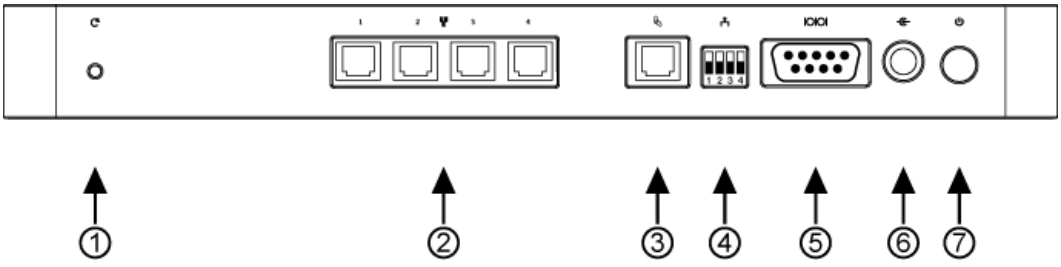
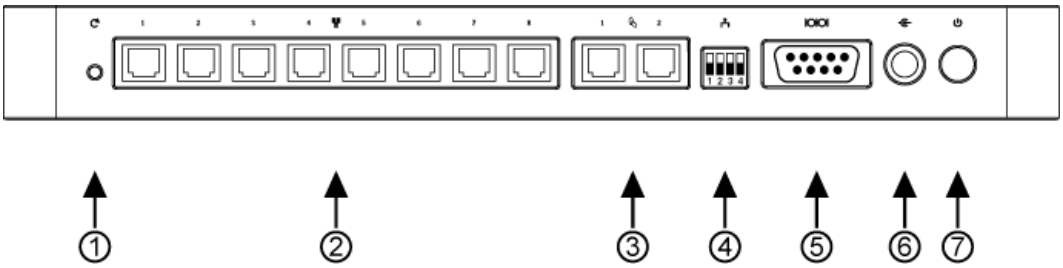


Figure 9-3 shows the rear panel of models 460 and 460R. This figure is for reference only; the full description of each feature is available in the *Symantec Gateway Security 400 Series Installation Guide*.

Figure 9-3 Models 460 and 460R rear panel



To flash the firmware

1. To turn off the power, press the power button on the back panel of the appliance.
2. Turn DIP switches 1 and 2 (4) to the on (up) position.
3. To turn on the power, press the power button (7).
4. Copy the firmware file and the symcftpw utility into a temporary folder on your hard drive.
5. Double-click the symcftpw icon.
6. In the Server IP text box, type the LAN IP address of the appliance.
   The default LAN IP address of the appliance is 192.168.0.1.
7. In the Local File text box, type a file name for the firmware upgrade file.
8. Click **Put**.
   Wait several minutes before restarting the appliance. Flashing is complete when symcftpw reports that flashing is complete, LEDs 2 and 3 stop flashing alternately, the appliance has restarted, and then LEDs 1 and 3 are illuminated steadily. This may take several minutes.
9. Turn DIP switches 1 and 2 (4) to the off position (down).

Running LiveUpdate Now

Run LiveUpdate Now is the manual LiveUpdate feature. Run LiveUpdate Now immediately checks for the latest firmware updates for your appliance and installs it. If you are already running the latest version, it does not update your appliance. LiveUpdate updates retain your configuration.

You can also change the address of the LiveUpdate server to check. See "Changing the LiveUpdate server location" on page 98.

To run LiveUpdate now

See "Trusted Certificates tab field descriptions" on page 123.

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the LiveUpdate tab, under Status, click **Run LiveUpdate Now.**

Forcing a firmware update

If manually flashing the firmware does not work, you can force the firmware on to the appliance. Do this only if flashing firmware as instructed in "Flashing the firmware" on page 100 does not work, or if you are instructed to do so by Symantec Technical Support.

Use Figure 9-2 and Figure 9-3 for reference in the following procedure. Before you begin, note all of your configuration settings.

To force a firmware update

1. To turn off the power, press the power button on the back panel of the appliance.
2. Turn DIP switches 2 and 4 (4) to the on (up) position.
3. To turn on the power, press the power button (7).
4. On the LAN computer from which you will TFTP the firmware to the appliance, change its IP address to a static IP address outside the default IP address range (192.168.0.2-1.92.168.0.52).
   Also, do not give the computer the static IP address 192.168.0.1.
5. Copy the firmware file and the symcftpw utility into a temporary folder on your hard drive.
6. Double-click the symcftpw icon.
7. In the Server IP text box, type the LAN IP address of the appliance.
   The default LAN IP address of the appliance is 192.168.0.1.
8. In the Local File text box, type a file name for the firmware upgrade file.
9. Click **Put**.
   Wait several minutes before restarting the appliance. Flashing is complete when symcftpw reports that flashing is complete, LEDs 2 and 3 stop flashing alternately, the appliance has restarted, and then LEDs 1 and 3 are illuminated steadily. This may take several minutes.
10. Turn DIP switches 2 and 4 (4) to the off position (down).

Checking firmware update status

The Status section shows the date and version of the last firmware update. The last update shows the date and time (if an NTP service is available) of the last LiveUpdate check. This check may or may not have resulted in a new firmware version being downloaded depending on whether the appliances firmware is already the most recent version.

For automatic updates, LiveUpdate logs messages for the following events:

- Successfully downloading the firmware package
- Unsuccessfully downloading the firmware package
- No new firmware package available; every component is current

If a LiveUpdate fails because of an HTTP error, the failure is logged along with the HTTP error message reported by the HTTP client.

To check firmware update status

It is important to know the version of the firmware on the appliance if you plan to contact Symantec Technical Support.

See "Status tab field descriptions" on page 118.

To view LiveUpdate firmware package status

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the LiveUpdate tab, under Status, view the date of the last update and the version number.

To view the current version of the firmware on the appliance

1. In the SGMI, in the left pane, click **Logging/Monitoring**.
2. In the right pane, on the Status tab, under Unit, view the Firmware Version.

Backing up and restoring configurations

You can back up your appliance configuration at any time. You should do this after you initially configure the appliance or before changing the configuration significantly.

Note: You should not use a configuration backup file from an older version of the firmware to restore your settings unless instructed to do so by Symantec Technical Support.

The backup file is created in the same folder on your hard drive where you put the symcftpw application. In the symcftpw application, you can specify where to store the backup file, such as a a floppy disk. This is useful to store the configuration in a safe location, such as a fire-safe box.

To back up and restore configurations

Backing up your configuration is good practice to ensure that you can restore the configuration if the appliance fails.

To back up an appliance configuration

1. To turn off the power, press the power button on the back panel of the appliance.
2. Turn DIP switches 1 and 2 to the on (up) position.
3. Turn on the appliance by pressing the power button.
4. Copy the symcftpw utility from the product CD-ROM to a folder on your hard drive.
5. Double-click the symcftpw icon.
6. In the Server IP text box, type the LAN IP address of the appliance.
   The default LAN IP address of the appliance is 192.168.0.1.
7. In the Local File text box, type the file name of the backup file.
8. Click **Put**.
9. Turn DIP switches 1 and 2 to the off (down) position.
10. Copy the backup file from your hard drive to a floppy disk and store in a secure location.

To restore an appliance configuration

1. To turn off the power, press the power button on the back panel of the appliance.
2. Turn DIP switches 1 and 2 to the on (up) position.
3. Turn on the appliance by pressing the power button.
4. Copy the symcftpw utility from the product CD-ROM to a folder on your hard drive.
5. Double-click the symcftpw icon.
6. In the Server IP text box, type the LAN IP address of the appliance.
   The default LAN IP address of the appliance is 192.168.0.1.
7. In the Local File text box, type a file name for the backup file.
8. Click **Get**.
9. Turn DIP switches 1 and 2 to the off (down) position.

Resetting the appliance

You can reset the appliance in three different ways:

- Basic reset
  Restarts the appliance. This is similar to turning off and then turning on the appliance. All current connections, including client VPN tunnels, are lost. Previously connected gateway-to-gateway VPN tunnels are reestablished when the appliance restarts. Also, the appliance performs a self-test of the hardware when the appliance restarts.
- Reset to the default configuration
  The LAN subnet IP address is reset to 191.168.0.0, the LAN IP address of the appliance is reset to 192.168.0.1, the DHCP server functionality is enabled, and the administrator's password is reset to blank.
- Reset to the reserved application
  The firmware resets to the last all.bin firmware file that was used to flash the appliance. This is either the factory firmware or a firmware upgrade that you downloaded from the Symantec Web site and applied to the appliance.

Note: LiveUpdate does not download and apply all.bin firmware upgrades.

To reset the appliance

There are three types of factory reset, which you can perform using a combination of the DIP switches and the reset button. You must use a paper clip or pen tip to press the reset button. Refer to Figure 9-4 and Figure 9-5 for the location of the reset button and DIP switches.

Figure 9-4 shows the rear panel of models 420 and 440 and Figure 9-5 shows the rear panel of models 460 and 460R. These figures are for reference only; the full description of each feature is available in the *Symantec Gateway Security 400 Series Installation Guide*.

Figure 9-4 Model 420 or 440 rear panel

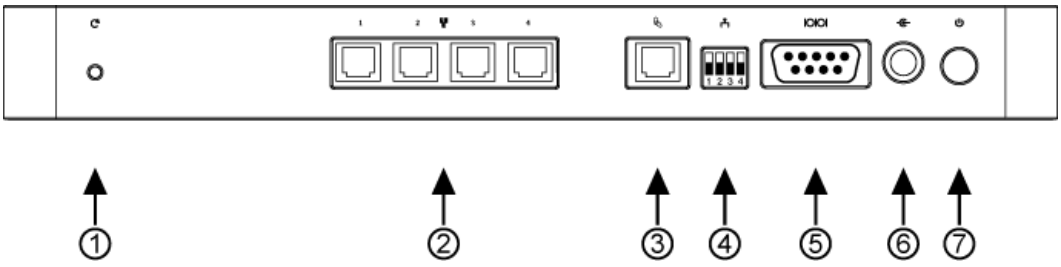
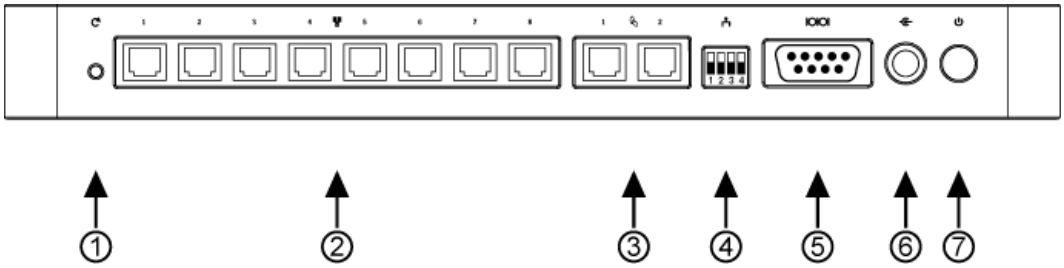


Figure 9-5 Model 460 and 460R rear panel



To perform a basic reset

- On the rear panel of the appliance, quickly press the reset button (1).

To perform a reset to the default configuration

- On the rear panel of the appliance, press and hold the reset button (1) for five seconds.

To perform a reset to the reserved application

1. On the rear panel of the appliance, turn DIP switch 4 (4) to the on position (up).
2. Quickly press the reset button (1).

Interpreting LEDs

The LEDs on the front of each appliance indicate the status of the appliance. There are six LEDs; four for the appliance, and two for wireless. The wireless LEDs generally only illuminate when a compatible Symantec Gateway Security WLAN Access Point option is inserted.

Figure 9-6 shows the front panel on all 400 Series appliances. This figure is for reference only; the full description of each feature is available in the *Symantec Gateway Security 400 Series Installation Guide*.

Figure 9-6 Symantec Gateway Security 400 Series appliance front panel

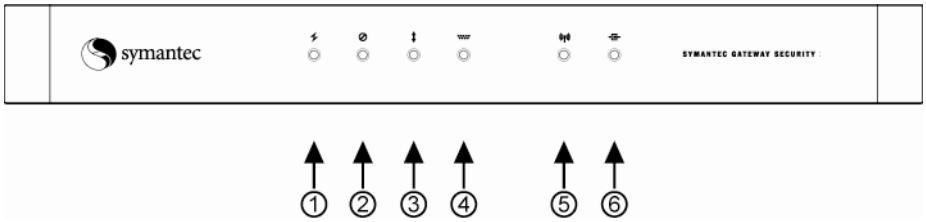


Table 9-2 describes each LED.

Table 9-2 LEDs

Location	Symbol	Feature	Description
1		Power	Illuminates when the appliance is turned on.
2		Error	Illuminates if there is a problem with the appliance.
3		Transmit	Illuminates or flashes when traffic is being passed over the LAN or WAN ports.
4		Backup	Illuminates or flashes when the serial port is being used or is not functioning correctly.
5		Wireless-ready	Illuminates when the wireless card is inserted and functioning properly.
6		Wireless-connect	Illuminates or flashes when at least one wireless client is connected.

The LEDs on the front panel of the appliance have three states: solid on, flashing, and solid off. The combination of the Error and Transmit LED states indicate the status of the appliance. Table 9-3 describes the LEDs state combinations and appliance status that they indicate.

Table 9-3 LEDs states and appliance status

Error LED state	Transmit LED state	Appliance status
Solid off	Solid on	Normal operation.
Solid off	Flashing	Transmitting/receiving Data from LAN.
Flashing	Flashing	■ MAC address not assigned. ■ Firmware problem. Appliance is ready for a forced download. ■ Appliance detected an error and cannot recover.
Flashing	Solid on	Configuration mode.
Solid on	Solid on	Hardware problem.
Flashing once	Solid off	RAM error.
Flashing twice	Solid off	Timer error.
Flashing thrice	Solid off	DMA error.
Solid on	Flashing once	LAN error.
Solid on	Flashing twice	WAN error.
Solid on	Flashing thrice	Serial error.
Solid off	Solid off	No power.
Both flashing alternately		■ Download in progress. ■ Appliance is writing to flash.

LiveUpdate and firmware upgrade LED sequences

When you apply a firmware upgrade using the symcftpw utility or TFTP, or if LiveUpdate is downloading and applying a firmware upgrade, there is a unique sequence of LED flashing that indicates the progress. Table 9-4 describes the sequences.

Table 9-4 LiveUpdate LED sequences

Description	Power	Error	Transmit
Firmware retrieval from the Internet using LiveUpdate or uploading it using the symcftpw or TFTP tools.	On	On	Flashing when there is traffic.
Firmware downloaded and verified. This takes approximately 10 seconds.	On	Off	Off
Applying the firmware. The amount of time this takes depends on the model.	On	Flashing alternately with Transmit.	Flashing alternately with Error.
Update complete.	On	On	On
Appliance resets, all LEDs illuminate, and then go to the normal operation pattern.	On	Off	Flashing when there is traffic.

Appendix A

Troubleshooting

This chapter includes the following topics:

- About troubleshooting
- Accessing troubleshooting information

About troubleshooting

The Debug information feature provides a high level of detail of the system events information in the log. Debug mode gives more detailed information in the status log that is useful for Symantec Technical Support or for troubleshooting. The default user mode provides general information about actions taken defined by the security policy.

Warning: Enabling debug mode increases the number of log events and impacts performance. By design, all debug messages are in English only. Only use debug mode temporarily for troubleshooting purposes, and disable it immediately after debugging.

The Forward WAN packets to LAN feature broadcasts all WAN side packets into the LAN for packet capturing (sniffing). This is a potential security issue, so ensure that you disable this feature when you are done troubleshooting.

The security gateway also provides both PING and DNS Lookup testing tools to verify network connectivity and DNS resolution.

Note: The PING troubleshooting tool should only be used to issue PING commands to other IP addresses; you cannot PING the appliance itself.

The Result section of the Troubleshooting window shows the result of running a PING or DNS Lookup test.

To troubleshoot Symantec Gateway Security 400 Series appliances

See "Logging/Monitoring field descriptions" on page 117.

See "Troubleshooting tab field descriptions" on page 121.

To set logging levels

1. In the SGMI, in the left pane, click **Logging/Monitoring**.
2. In the right pane, on the Log Settings tab, under Log Type, check the information to log.
   Debug information captures a great deal of information. Use this option only during troubleshooting.
3. Click **Save**.

To enable forward WAN packets to LAN

1. In the SGMI, in the left pane, click **Logging/Monitoring**.
2. In the right pane, on the Troubleshooting tab, under Broadcast Debug Level, check **Forward WAN packets to LAN**.
   Forwarding packets received on the WAN ports to the LAN for troubleshooting purposes may allow traffic normally denied by the security gateway into your internal network. You should only use this method for capturing WAN packets if you are unable to use a sniffer in the WAN side of your network. Only enable this feature as a last resort, and turn it off immediately once you finish troubleshooting.
3. Click **Save**.

To run a test

1. In the SGMI, in the left pane, click **Logging/Monitoring**.
2. In the right pane, on the Troubleshooting tab, under Testing Tools, in the **Target Host** text box, type the IP address or DNS name you want to test.
3. In the Tool drop-down list select **PING** or **DNS Lookup**.
4. Click **Run Tool**.

The results of the test display under Result.

To test default gateway connectivity

1. Verify that your default gateway is reachable by issuing a PING request to its IP address.
2. If you can not PING a host by its IP address you either have an ISP link problem or a routing problem.
3. If you can PING a host by IP address but not by DNS name, you have a DNS server misconfiguration or the DNS server is not reachable (try to PING the DNS server by IP address to verify connectivity).
4. If you can successfully resolve some DNS names but not others, the most likely problem is not your configuration. In this case you will have to work with the authoritative source for that DNS domain to resolve the problem.

To test WAN connectivity

1. PING the default gateway.
2. PING an Internet site by its IP address.
3. PING an Internet site by its DNS address.

Note: Some sites block PINGs on their firewalls. Make sure the site is reachable before calling your ISP or Symantec Technical Support.

Accessing troubleshooting information

Use the following procedure to access troubleshooting information from the Symantec Knowledge Base.

To access troubleshooting information

1. Go to www.symantec.com.
2. On the top of the home page, click **support.**
3. Under Product Support > enterprise, click **Continue.**
4. On the Support enterprise page, under Technical Support, click **knowledge base**.
5. Under select a knowledge base, scroll down and click **Symantec Gateway Security 400 Series**.

6 Click your specific product name and model.

7 On the knowledge base page for your appliance model, do any of the following:

- On the Hot Topics tab, click any of the items in the list to view a detailed list of knowledge base articles on that topic.
- On the Search tab, in the text box, type a string containing your question. Use the drop-down list to determine how the search is performed and click **Search**.
- On the Browse tab, expand a heading to see knowledge base articles related to that topic.

Appendix B

Licensing

This chapter includes the following topics:

- SYMANTEC GATEWAY SECURITY APPLIANCE (300/400 SERIES) LICENSE AND WARRANTY AGREEMENT
- SYMANTEC GATEWAY SECURITY APPLIANCE (300/400 SERIES) CLIENT-TO-GATEWAY VPN ADDITIVE LICENSE AND 8.0 MEDIA KIT

SYMANTEC GATEWAY SECURITY APPLIANCE (300/400 SERIES) LICENSE AND WARRANTY AGREEMENT

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE INCLUDED WITH THE APPLIANCE YOU HAVE PURCHASED TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") AND TO PROVIDE WARRANTIES ON THE APPLIANCE ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AND WARRANTY AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AND WARRANTY AGREEMENT CAREFULLY BEFORE USING THE APPLIANCE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, REQUESTING A LICENSE KEY OR USING THE SOFTWARE AND THE APPLIANCE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE" OR "NO" BUTTON IF APPLICABLE AND DO NOT USE THE SOFTWARE AND THE APPLIANCE.

1. Software License:

The software (the "Software") which accompanies the appliance You have purchased (the "Appliance") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Appliance and/or the Software, Your rights and obligations with respect to the use of this Software are as follows:

You may:

A._____ use the Software solely as part of the Appliance.

B. _____ make copies of the printed documentation which accompanies the Appliance as necessary to support Your authorized use of the Appliance; and

C. _____ after written notice to Symantec and in connection with a transfer of the Appliance, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies

of the Software, Symantec consents to the transfer and the transferee agrees in writing to the terms and conditions of this agreement.

You may not:

A. _____ sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

B. _____ use, if You received the Software distributed on an Appliance containing multiple Symantec products, any Symantec software on the Appliance for which You have not received a permission in a License Module; or

C. _____ use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Symantec software products utilize content that is updated from time to time (e.g., antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; some firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for each Software functionality which You have purchased and activated for use with the Appliance for any period for which You have (i) purchased a subscription for Content Updates for such Software functionality; (ii) entered into a support agreement that includes Content Updates for such Software functionality; or (iii) otherwise separately acquired the right to obtain Content Updates for such Software functionality. This license does not otherwise permit You to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the Software will perform on the Appliance in substantial compliance with the written documentation accompanying the Appliance for a period of thirty (30) days from the date of original purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, repair or replace any defective Software returned to Symantec within the warranty period or refund the money You paid for the Appliance.

Symantec warrants that the hardware component of the Appliance (the “Hardware”) shall be free from defects in material and workmanship under normal use and service and substantially conform to the written documentation accompanying the Appliance for a period of three hundred sixty-five (365) days from the date of original purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, repair or replace any defective Hardware returned to Symantec within the warranty period or refund the money You paid for the Appliance.

The warranties contained in this agreement will not apply to any Software or Hardware which:

A. _____ has been altered, supplemented, upgraded or modified in any way; or

B. _____ has been repaired except by Symantec or its designee.

Additionally, the warranties contained in this agreement do not apply to repair or replacement caused or necessitated by: (i) events occurring after risk of loss passes to You such as loss or damage during shipment; (ii) acts of God including without limitation natural acts such as fire, flood, wind earthquake, lightning or similar disaster; (iii) improper use, environment, installation or electrical supply, improper maintenance, or any other misuse, abuse or mishandling; (iv) governmental actions or inactions; (v) strikes or work stoppages; (vi) Your failure to follow applicable use or operations instructions or manuals; (vii) Your failure to implement, or to allow Symantec or its designee to implement, any corrections or modifications to the Appliance made available to You by Symantec; or (viii) such other events outside Symantec’s reasonable control.

Upon discovery of any failure of the Hardware, or component thereof, to conform to the applicable warranty during the applicable warranty period, You are required to contact us within ten (10) days after such failure and seek a return material authorization (“RMA”) number. Symantec will promptly issue the

requested RMA as long as we determine that You meet the conditions for warranty service. The allegedly defective Appliance, or component thereof, shall be returned to Symantec, securely and properly packaged, freight and insurance prepaid, with the RMA number prominently displayed on the exterior of the shipment packaging and with the Appliance. Symantec will have no obligation to accept any Appliance which is returned without an RMA number.

Upon completion of repair or if Symantec decides, in accordance with the warranty, to replace a defective Appliance, Symantec will return such repaired or replacement Appliance to You, freight and insurance prepaid. In the event that Symantec, in its sole discretion, determines that it is unable to replace or repair the Hardware, Symantec will refund to You the F.O.B. price paid by You for the defective Appliance. Defective Appliances returned to Symantec will become the property of Symantec.

Symantec does not warrant that the Appliance will meet Your requirements or that operation of the Appliance will be uninterrupted or that the Appliance will be error-free.

In order to exercise any of the warranty rights contained in this Agreement, You must have available an original sales receipt or bill of sale demonstrating proof of purchase with Your warranty claim.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE APPLIANCE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software or the Appliance.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

6. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. Licensee agrees to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Appliance and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software and shall return the Appliance to Symantec. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

SYMANTEC GATEWAY SECURITY APPLIANCE (300/400 SERIES) CLIENT-TO-GATEWAY VPN ADDITIVE LICENSE AND 8.0 MEDIA KIT

DESCRIPTION	INCREMENTAL CONCURRENT SESSIONS LICENSED	SERIAL NUMBER OF APPLIANCE TO WHICH THIS LICENSE APPLIES
SYMANTEC GATEWAY SECURITY 300/400 SERIES APPLIANCE ("APPLIANCE") xx SESSION CLIENT-TO-GATEWAY VPN ADDITIVE LICENSE AND 8.0 MEDIA KIT	xx	_____ (To Be Completed by Licensee)

IMPORTANT: The concurrent sessions shall not be legally licensed or authorized for use unless and until Licensee enters the serial number of the applicable Appliance for which these concurrent sessions are licensed in the space provided on the face of this Additive License Certificate. This license does not require a serial number, a license key or registration to enable the concurrent sessions licensed hereunder to be used on the Appliance bearing the serial number set forth on the face of this Additive License Certificate.

AMENDMENT TO SYMANTEC SOFTWARE LICENSE AND WARRANTY

This is a legal agreement between the end user of the additive license (the "Licensee"), and Symantec Corporation and/or its subsidiaries ("Symantec") which amends the Symantec license and warranty agreement (also known as the end user license agreement or "EULA") contained in the original media pack(s) of the Symantec software product(s) (the "Software") listed on the face of this Additive License Certificate (the "Certificate"). Accordingly, this Certificate and the rights granted herein are only effective as to end users who have received a media pack of the Software listed on the face of this Certificate and who have agreed to the terms of the EULA contained in such pack. Please read this Certificate. By using and installing the Software, Licensee indicates its consent to the terms and conditions set forth below.

IF LICENSEE DOES NOT AGREE TO THESE TERMS, THEN SYMANTEC IS UNWILLING TO LICENSE ADDITIONAL COPIES OF THE SOFTWARE TO LICENSEE. EXCEPT AS EXPRESSLY SET FORTH IN THIS CERTIFICATE, ALL PROVISIONS OF THE EULA WILL BE APPLICABLE FOR ALL RIGHTS GRANTED UNDER THIS CERTIFICATE. ANY RIGHT TO RETURN THE SOFTWARE AND ANY RIGHT TO USE THE SOFTWARE ON HOME COMPUTERS THAT MAY BE CONTAINED IN THE EULA SHALL NOT APPLY TO THE RIGHTS GRANTED UNDER THIS CERTIFICATE.

1. GRANT OF LICENSE. Symantec grants to Licensee a nonexclusive, nontransferable license to install and use the quantity of each title of the Software and the related user documentation as are set forth opposite the name of such title on the face of this Certificate, solely on the Appliance bearing the serial number set forth on the face of this Certificate, under the terms and conditions of the EULA, solely for Licensee's own internal business purposes.

2. SOFTWARE INSTALLATION AND USE RESTRICTION. Licensee may install the Software authorized under section 1 of this Certificate, in object code form only, from the copy of the Software and user documentation contained in the original media pack of the Software obtained from Licensee's dealer, on an unlimited number of Licensee's client machines; provided however, that Licensee's use of the Software on such client machines is restricted by the total number of concurrent sessions legally licensed hereunder or pursuant to any License Module, as applicable, for the Appliance bearing the serial number set forth on the face of this Certificate. An auditor, selected by Symantec and reasonably acceptable to Licensee, may, upon reasonable notice and during normal business hours, but not more often than once each year, inspect Licensee's records in order to confirm the legal use of the Software. Symantec shall bear the costs of any such audit.

3. INTEGRATION. This Certificate and the EULA constitute the entire agreement between the parties pertaining to the subject matter hereof, and supersede any and all written or oral agreements with respect to such subject matter hereof, and supersede any and all written or oral agreements with respect to such subject matter.

Appendix C

Field descriptions

This chapter includes the following topics:

- Logging/Monitoring field descriptions
- Administration field descriptions
- LAN field descriptions
- WAN/ISP field descriptions
- Firewall field descriptions
- VPN field descriptions
- IDS/IPS field descriptions
- Antivirus Policy field descriptions
- Content Filtering field descriptions

Logging/Monitoring field descriptions

The security gateway provides configurable system logging features and tabs for viewing the system logs and monitoring system status. It also has built-in testing tools for troubleshooting and connectivity verification.

This section contains the following topics:

- Status tab field descriptions
- View Log tab field descriptions
- Log Settings tab field descriptions
- Troubleshooting tab field descriptions

Status tab field descriptions

The Status tab shows the current conditions and settings of the security gateway.

Table C-1 Status tab field descriptions

Section	Field	Description
WAN (External Port) (Single WAN port models) WAN 1 (External Port) (Dual WAN port models) WAN 2 (External Port) (Dual WAN port models)	Connection Status	Displays whether the WAN port is connected or disconnected to the Internet or an internal network.
	Netmask	Derived from Dynamic Host Configuration Protocol (DHCP) or static IP configuration.
	IP Address	Displays the IP address of the WAN port based on your local configuration.
	Physical Address	Media Access Control (MAC) address of the security gateway.
	Default Gateway	Displays an IP address based on your local configuration. Used by the security gateway to route any packets destined to any networks it does not recognize. In most configurations, this is the IP address of your ISP's router.
	DHCP Client	Displays enabled or disabled. If enabled, the security gateway uses DHCP to request an IP address, DNS server, and routing information from your ISP or intranet when you start the security gateway.
	DNS IP Address(es)	Displays an IP address provided by your ISP.
	DHCP Lease Time	If DHCP Client is enabled, this displays the amount of time the security gateway will own the IP address. This is obtained when you start the security gateway.
LAN (External Port)	IP Address	Displays the IP address of the security gateway. The default value is 192.168.0.1.
	Physical Address	Displays the physical address (MAC) of the security gateway's LAN port. The default value is the factory setting.
	Netmask	Displays the network mask address as set on the LAN tab. The default value is 255.255.255.0.
	DHCP Server	Displays enabled or disabled, depending on whether the security gateway acts as a DHCP server for connected clients.

Table C-1 Status tab field descriptions (Continued)

Section	Field	Description
Unit	Firmware Version	Displays the factory firmware version or the firmware version from the most recent LiveUpdate or manual update.
	Language Version	Displays the factory version or the most recent update.
	Model	Displays the model number of the security gateway.
	Exposed Host	Displays enabled if you have enabled a computer on your network as an exposed host.
	Special Applications	Displays enabled or disabled. If you have configured any special applications, this field displays enabled.
	NAT Mode	Displays enabled or disabled. If you disable NAT mode, this disables the firewall security functions and the security gateway behaves as a standard router. Only use this setting for intranet security gateway deployments where, for example, the security gateway will be used as a wireless bridge on a protected network. When NAT mode is enabled (the default), the security gateway behaves as a 802.1D network bridge device.
SESA	Status	Displays Deactivated or Activated.
	SESA ID	If the SESA Status is Activated, the SESA ID is displayed here.
	Policy	Displays the Policy associated with the Organizational Unit of which the appliance is a member.
	Location	Displays the Location Settings associated with the Organizational Unit of which the appliance is a member.
	Policy Revision	Displays the revision level of the policy.
	Location Revision	Displays the revision level of the location settings.

View Log tab field descriptions

The View Log tab shows a list of system events.

Table C-2 View Log field descriptions

Section	Field	Description
Log	UTC Time	Coordinated Universal Time (UTC), which is the Greenwich Mean Time that the message was logged. If the security gateway cannot obtain the current time from a network time protocol (NTP) server, it displays the number of seconds from when the security gateway was last restarted for each event.
	Message	Displays the text of the logged event.
	Source	Displays the origin of the packet.
	Destination	Displays the intended destination of the packet.
	Note	Displays the protocol name or number or additional troubleshooting information.

Log Settings tab field descriptions

The Log Settings tab lets you configure settings that control email notification, the types of messages that are logged, and the time listed for each log message.

Table C-3 Log Settings field descriptions

Section	Field	Description
Email Forwarding	SMTP Server	IP address or fully qualified domain name of the SMTP server to use to send the log. To email logs, this is a required field.
	Send Email From	Sender's email address. The maximum number of characters is 39. To email logs, this is a required field.
	Send Email To	Receiver's email address. The maximum number of characters is 39. Include multiple receivers by separating each address with a comma. To email logs, this is a required field.
	Email Log Now	After you have typed the SMTP server, and the sender and receiver email addresses, you can click Email Log Now to send an email of the most current log.
Syslog	Syslog Server	IP address of a host running a standard Syslog utility that can receive the log file.
Log Type	System activity, connection status	Logs all system activity and connection status. This type is checked by default.
	Connections ALLOWED by outbound rules	Logs all connections allowed by outbound rule policies.
	Connections DENIED by outbound rules	Logs all attempted connections denied by an outbound rule policy, antivirus policy enforcement (AVpe), and content filtering.
	Connections ALLOWED by inbound rules	Logs all connections allowed by inbound rules.
	Connections DENIED by inbound rules	Logs all attempted connections denied by inbound rules.
	Detected attack	Logs all detected attacks, including port scanning, fragmentation, and Trojan horse attacks. This type is checked by default.
	Debug information	Displays additional debug information that is useful for troubleshooting. Only use this option when you are troubleshooting a problem, and then disable it after you have solved the problem.
Time	NTP Server	IP address of the non-public Network Time Protocol (NTP) Server.

Troubleshooting tab field descriptions

The Troubleshooting tab helps you troubleshoot your security gateway with debug options, and testing tools.

Table C-4 Troubleshooting tab field descriptions

Section	Field	Description
Broadcast Debug Level	Forward WAN packets to LAN	Enables forwarding of WAN packets to LAN. This is useful to check the WAN packets for troubleshooting without having to set up additional equipment.
Testing Tools	Target Host	IP address or fully qualified domain name of host you are testing with one of the tools. The address is not validated, so ensure that you type the address accurately.
	Tool (Single WAN port models)	Troubleshooting tools. Options include: ■ PING ■ DNS Lookup Click Run Tool to start the troubleshooting tool.
	Tool (Dual WAN port models)	Troubleshooting tools. Options include: ■ PING ■ DNS Lookup Click Run thru WAN 1 or Run thru WAN 2, depending which WAN port you want to troubleshoot.
Result	Result	Displays result of tool test.

Administration field descriptions

The Administration feature of the security gateway lets you manage administrator access to the SGMI with a password and allowed IP addresses. You can also configure SNMP for system monitoring and LiveUpdate to receive firmware updates.

This section contains the following topics:

■ Basic Management tab field descriptions
■ Advanced Management tab field descriptions
■ SNMP tab field descriptions
■ Trusted Certificates tab field descriptions
■ LiveUpdate tab field descriptions

Basic Management tab field descriptions

The Basic Management tab helps you control access to the SGMI with the administration password and allowed IP addresses.

Table C-5 Basic Management tab field descriptions

Section	Field	Description
Administration Password	admin's Password	Password used to access the SGMI. The user name is always admin. The login is case-sensitive.
	Verify Password	Retype the admin's password.

Table C-5 Basic Management tab field descriptions (Continued)

Section	Field	Description
Remote Management	Start IP Address	First IP address in the range of addresses that you permit to access the SGMI. To delete an IP address, enter 0 in each of the text boxes.
	End IP Address	Last IP address in the range of addresses that you permit to access the SGMI. To delete an IP address, enter 0 in each of the text boxes.
	Allow Remote Firmware Upgrade	Allows a firmware upgrade from the range of IP addresses.

Advanced Management tab field descriptions

The Advanced Management tab lets you configure your security gateway to be managed by the Symantec Management Console.

Table C-6 Advanced Management tab field descriptions

Section	Field	Description
Centralized Management	Management Mode	Select one of these management modes: ■ Centralized Monitoring and Policy Management Select this option when joining SESA for Advanced Management. ■ Centralized Monitoring (Alerting, Logging, and Reporting) Select this option when joining SESA for Event Management. ■ Standalone Management Manage the appliance locally. If this option is selected when you try to join SESA, an error is displayed.
Symantec Enterprise Security Architecture (SESA) Registration	Bind to WAN Port (Dual WAN port models)	The port through which the gateway should connect to the SESA Manager. Valid values are WAN 1 or WAN 2.
	Management Server	IP address or fully-qualified domain name of the SESA management server.
	Administrator	The administrator's login name.
	Password	The administrator password.
	Query SESA	Click Query SESA to populate the drop-down list of organizational units configured on the SESA server.
	Organizational Unit	The SESA organizational units configured on the SESA server.
	Join SESA	Click here to join the security gateway to the specified SESA Manager.
	Disconnect SESA	Click here to temporarily leave SESA management while leaving the SESA configuration intact.
	Reconnect SESA	Click here to reconnect to the Symantec Management Console. A message warns that any configuration changes made while in local management mode may be overwritten.
	Leave SESA	Click here to remove the security gateway from SESA management mode permanently. To go back to SESA management, you must join SESA again.

Table C-6 Advanced Management tab field descriptions (Continued)

Section	Field	Description
Local SESA Agent Status	Refresh	Click Refresh to refresh the Local SESA Agent Status.
	Get Configuration	Click Get Configuration to download the configuration from the organizational unit selected above.
	At the bottom of the screen, you can view SESA Agent status information, including SESA mode, SESA server, SESA ID, and other status information.	

SNMP tab field descriptions

The SNMP tab lets you configure your security gateway to be monitored by SNMP servers.

Table C-7 SNMP tab field descriptions

Section	Field	Description
SNMP Read-only Managers (GETS and TRAPS)	Community String	A community string may be required by your SNMP server.
	IP Address 1, IP Address 2, IP Address 3	IP address of SNMP TRAP receivers. TRAPs are forwarded to these addresses.
	Enable Remote Monitoring	Allows external access to SNMP GET on the appliance.

Trusted Certificates tab field descriptions

The Trusted Certificates tab lets you view status information about certificates being used on the security gateway.

Table C-8 Trusted Certificates field descriptions

Section	Field	Description
Trusted Root Certificate Authorities	Certificate Issued To	Host to whom the certificate was issued.
	Certificate File Location	Click Browse to browse to the location in which the certificate is stored.
	View	Click here to view the certificate information.
	Import	Click here to import the certificate.
	Delete	Click here to delete the certificate.

Table C-8 Trusted Certificates field descriptions (Continued)

Section	Field	Description
Certificate Attributes	Certificate Issued To	Owner of the certificate.
	Certificate Issued By	Certificate authority that issued the certificate.
	Version	Version of the certificate.
	Issuer DN	Distinguished Name of the certificate issuer.
	Subject DN	Distinguished Name of the certificate subject.
	Subject Email	Email address of certificate subject.
	Not Valid Before	First day/time of certificate validity.
	Not Valid After	Certificate expiration date/time.
	Distribution Point	Certificate distribution point.
	Sign Algorithm	Certificate signature algorithm.
	Serial Number	Certificate serial number (16 two-digit hex numbers).
	Fingerprint	Certificate fingerprint (20 two-digit hex numbers).

LiveUpdate tab field descriptions

The LiveUpdate tab lets you configure your connection to a LiveUpdate server and schedule firmware updates for your security gateway.

Table C-9 LiveUpdate tab field descriptions

Section	Field	Description
General Settings	LiveUpdate Server	IP address or fully qualified domain name of the LiveUpdate server from which to get firmware updates. The default address is http://liveupdate.symantec.com.
Automatic Updates	Enable Scheduler	Enables the LiveUpdate scheduler. This lets you schedule times for the security gateway to automatically check for firmware updates, and then apply them.
	Frequency	Frequency with which the security gateway checks for updates. The start time for the frequency is based on the most recent reboot of the appliance. Options include: ■ Daily ■ Weekly ■ Bi-weekly ■ Monthly
	Preferred Time (UTC)	Time in hours and minutes at which the security gateway automatically checks for updates. The format is HH:MM, where HH is hours between 0 and 24, and MM is minutes between 0 and 59. For example, to check for updates at 7:30 pm, type 19:30. The UTC setting is dependent on access to an NTP server. Use only numeric characters and a colon in this text box.

Table C-9 LiveUpdate tab field descriptions (Continued)

Section	Field	Description
Optional Settings	HTTP Proxy Server	Enables the security gateway to contact the LiveUpdate server through a HTTP proxy server.
	Proxy Server Address	IP address of the HTTP proxy server through which the LiveUpdate server gets the firmware updates.
	Port	Port number associated with the HTTP proxy server through which the LiveUpdate server gets the firmware update. The maximum value is 65535. The default port is 80.
	User Name	User name associated with the HTTP proxy server through which LiveUpdate gets the firmware update.
	Password	Password associated with the HTTP server.
Status	Last Update	Date of the most recent update (in format YYYYMMDD).
	Last Update Version	Version number of the most recent update.

LAN field descriptions

LAN settings let you configure your security gateway to work in a new or existing internal network. LAN settings include the security gateway's IP address, whether it acts as a DHCP server for the nodes it protects, and LAN port settings.

This section contains the following topics:

- LAN IP & DHCP tab field descriptions
- Port Assignments tab field descriptions

LAN IP & DHCP tab field descriptions

The LAN IP & DHCP tab lets you set the security gateway's IP address and configure the security gateway to act as a DHCP server.

Table C-10 LAN IP & DHCP tab field descriptions

Section	Field	Description
LAN IP	IP Address	IP address of the security gateway's internal interface. The current IP address appears in the text boxes. The default value is 192.168.0.1. You cannot set the security gateway's IP address to 192.168.1.0.
	Netmask	Security gateway netmask. The current netmask appears in the text boxes. The default value is 255.255.255.0.

Table C-10 LAN IP & DHCP tab field descriptions (Continued)

Section	Field	Description
DHCP	DHCP Server	Clicking Enable makes the security gateway act as a DHCP server. To use another DHCP server, or if the clients use static IP addresses, click Disable.
	Range Start IP Address	First IP address in the range of IP addresses that you want the security gateway to assign to clients. For example, if you want the security gateway to assign IP addresses in the range 172.16.0.2 to 172.16.0.75, in the Range Start IP Address text boxes, type 172.16.0.2.
	Range End IP Address	Last IP address in the range of IP addresses that you want the security gateway to assign to clients. In the previous example, type 172.16.0.75 in the Range End IP Address text boxes.
DHCP Table	Host Name	Name of the computer to which the security gateway assigned an IP address.
	IP Address	IP address from the indicated range that the security gateway assigned to the computer.
	Physical Address	Physical (MAC) address of the network interface card (NIC) in the computer that was assigned an IP address.
	Status	Status of the DHCP lease on the IP address that was assigned to the computer. The options are: ■ Leased ■ Reserved

Port Assignments tab field descriptions

Port assignments let you specify if the LAN port resides on a trusted or untrusted virtual LAN (VLAN). The trusted VLAN is for wired connections and the non-trusted is for wireless connections.

Table C-11 Port Assignment tab field descriptions

Section	Field	Description
Physical LAN Ports	Port 1, Port 2, Port 3, Port 4 (Single WAN port models) Port 1, Port 2, Port 3, Port 4, Port 5, Port 6, Port 7, Port 8 (Dual WAN port models)	Assigns ports on the switch function of the security gateway as trusted or untrusted. This enables wireless and wired LAN-based VPN security through the port-based virtual network capabilities of the switch function on the security gateway, in addition to support for LAN-side global tunnels directly to the wireless interface. The tunnel endpoint will be at the main gateway for each LAN network subnet. Options include: ■ Standard Use this assignment for all wired LAN devices. All traffic is implicitly trusted and allowed to pass between VLANs. ■ SGS Access Point Secured Enables VPN security to be enforced at the roaming access point or switch level. ■ Enforce VPN tunnels/Allow IPSec pass-thru Explicit untrusted association. Requires a mandatory VPN tunnel between the wireless VPN client and the security gateway. IPsec traffic is allowed to pass through a subsidiary switch with tunnel termination points located at the primary security gateway and the client.

WAN/ISP field descriptions

The Symantec Gateway Security 300/400 Series WAN/ISP functionality provides connections to the outside world. This can be the Internet, a corporate network, or any other external private or public network. You can also configure the WAN port to connect to an internal LAN when the security gateway is protecting an internal subnet.

This section contains the following topics:

■ Main Setup tab field descriptions
■ Static IP & DNS tab field descriptions
■ PPPoE tab field descriptions
■ Dial-up Backup & Analog/ISDN tab field descriptions
■ PPTP tab field descriptions
■ Dynamic DNS tab field descriptions
■ Routing tab field descriptions
■ Advanced tab field descriptions

Main Setup tab field descriptions

On the Main Setup tab, you select your connection type and configure the security gateway's identification settings.

Table C-12 Main Setup tab field descriptions

Section	Fields	Description
Connection Type (Single WAN port models) WAN1 (External) or WAN2 (External) (Dual WAN port models)	Connection Type	The following connection types are supported: ■ DHCP (Auto IP) Your ISP assigns you an IP address automatically each time you connect. ■ PPPoE Point-to-Point Protocol over Ethernet (PPPoE) is a specification for connecting the users on an Ethernet LAN to the Internet. ■ Analog or ISDN Dial-up account. ■ Static IP Your ISP assigns or you have purchased a permanent IP address. ■ PPTP Your ISP uses Point-to-Point Tunneling Protocol (PPTP).
	HA Mode (Dual WAN port models)	The following high availability modes are available for the WAN ports: ■ Normal Load balancing settings apply to the port when it is enabled and operational. ■ Off The WAN port is not used at all. ■ Backup The WAN port only passes traffic if the other WAN port is not functioning.
	Alive Indicator Server (Dual WAN port models)	URL for a site to which the security gateway sends a PING or echo request to test for connectivity. If you do not specify a URL, the security gateway uses the address of the default gateway.
Optional Network Settings	Host Name	Name of the security gateway on the network. A default value based on the model number and the MAC address is provided in the Setup Wizard.
	Domain Name	Domain name by which external users can access the security gateway. For example, mysite.com.
	MAC Address	Physical (MAC) address of the security gateway. The default value is set at the factory. You can change this value if your ISP is expecting a certain MAC address (MAC spoofing or cloning).

Static IP & DNS tab field descriptions

Use the Static IP & DNS tab to configure the security gateway to connect to the Internet with a static IP address and DNS servers, or to connect to your intranet.

Table C-13 Static IP and DNS tab field descriptions

Section	Field	Description
WAN IP (Single WAN port models) WAN 1 IP, WAN 2 IP (Dual WAN port models)	IP Address	Static IP address for your account. If you type an IP address, you must also type a netmask and a default gateway.
	Netmask	Netmask for your account. The netmask determines if packets are sent to the default gateway. If you type a netmask, you must also type an IP address and a default gateway.
	Default Gateway	IP address of the default gateway. The security gateway sends any packet it does not know how to route to the default gateway. If you type a default gateway, you must also type an IP address and a netmask.
Domain Name Servers	DNS 1, DNS 2, DNS 3	You must specify at least one, and up to three, DNS servers to use for resolving host and IP addresses.

PPPoE tab field descriptions

Use the PPPoE tab to configure the security gateway to connect to the Internet with an account that uses PPPoE for authentication.

Table C-14 PPPoE tab field descriptions

Section	Field	Description
Sessions (Single WAN port models)	WAN Port (Dual WAN port models)	Select the WAN port for which you are configuring PPPoE.
Port and Sessions (Dual WAN port models)	Session	Lets you configure how the WAN port uses PPPoE. To configure a single-session PPPoE account, click Session 1, and then click Select. To configure a multi-session PPPoE account, select the session to configure, and then click Select.

Table C-14 PPPoE tab field descriptions (Continued)

Section	Field	Description
Connection	Connect on Demand	Lets the security gateway create a connection to the PPPoE account only when an internal user makes a request, such as browsing to a Web page. This field, combined with Idle Time-out, is useful if your ISP charges are on a per-usage time basis.
	Idle Time-out	Number of minutes that the connection can remain idle (unused) before disconnecting. Type 0 to keep the connection always on and to prevent the security gateway from disconnecting. If the value is more than 0, check the Connect on Demand check box to reconnect automatically when needed. When combined with Connect on Demand, the connection to your ISP is only made when a client is using it.
	Static IP Address	If you received a static IP address for your PPPoE account from your ISP, type it here.
Choose Service	Query Services	When you click Query Services, the security gateway connects to your ISP and determines which services are available. You must disconnect from your PPPoE account before using this feature.
	Service	Select a service for the PPPoE account. To determine the services that are available, click Query Services.
User Information	User Name	User name for the PPPoE account. This may be different from the account name. Some ISPs expect email address format for the user name, for example, johndoe@myisp.net.
	Password	Password for the PPPoE account.
	Verify Password	Retype the password for the PPPoE account.
Manual Control	Connect	Create a connection to the PPPoE account.
	Disconnect	Closes an open connection to the PPPoE account.

Dial-up Backup & Analog/ISDN tab field descriptions

The Dial-Up Backup & Analog/ISDN tab lets you configure the security gateway to connect to the Internet with a primary dial-up account, a primary dial-up ISDN account, or a back-up dial-up account.

Table C-15 Dial-up or ISDN tab field descriptions

Section	Field	Description
Backup Model	Enable Backup Mode	If you use a dedicated account as your primary connection, you can check Enable Backup Mode to automatically re-connect if the connection to the account fails.
	Alive Indicator Site IP or URL	IP address or URL to which to connect in the event of a connection failure.

Table C-15 Dial-up or ISDN tab field descriptions (Continued)

Section	Field	Description
ISP Account Information	User Name	User name for the dial-up account.
	Password	Password for the dial-up account.
	Verify Password	Retype the password for the dial-up account.
	IP Address	If you have a static IP address with your ISP, type it here; otherwise, the ISP dynamically assigns you an IP address.
	Dial-up Telephone 1, Dial-up Telephone 2, Dial-up Telephone 3	Telephone number for the security gateway to dial to connect to the dial-up account. You must specify at least one, and up to three dial-up numbers. If Dial-up Telephone 1 fails to connect, the security gateway then dials Dial-up Telephone 2, and so on. If the security gateway must dial a 9 to get an outside line, type 9 and then a comma before the telephone number. For example: 9,18005551212. This text box allows numbers, commas, and spaces.
Modem Settings	Model	Model type of your modem. If your specific model type is not listed, click Other.
	Initialization String	Modem command that the security gateway sends to the modem to begin dialing the ISP. Specify this value only if you select Other as the modem model.
	Line Speed	The speed at which you want the modem to connect to the dial-up account. If the security gateway is having trouble connecting, lower the line speed.
	Line Type	The type of line for your account. ■ Dial Up Line This line type is typically used if a connection to the Internet is not connected all the time. ■ Leased line This line type provides a permanent connection to the Internet.
	Dial Type	The type of signal your modem uses to dial the dial-up telephone number. The options include: ■ pulse ■ tone ■ other
	Dial String	Modem command to begin dialing the dial-up telephone number.
	Idle Time-out	Number of minutes that the connection may remain idle (unused) before disconnecting.
	Redial String	Modem command that specifies to redial the dial-up telephone number if the initial connection fails.
Manual Control	Dial	Opens a connection to the dial-up account.
	Hang Up	Closes an open connection to the dial-up account.

Table C-15 Dial-up or ISDN tab field descriptions (Continued)

Section	Field	Description
Analog Status	Port Status	Describes the status of the serial port on the security gateway where the modem is connected. Possible port status values include: ■ Idle ■ Dialing ■ Internet Access ■ Hanging Up
	Physical Link	Indicates whether the modem is connected to the phone number. Possible physical link status values include: ■ Off ■ On
	PPP Link	Possible PPP link status values include: ■ User Authenticated via PPP (User name/password was correct) ■ Off ■ On
	PPP IP Address	IP address that is assigned to your account when you connect. If you have a static IP address, it is the same each time. If the ISP assigns IP addresses dynamically, the IP address may be different each time a connection is established. Possible PPP IP address values include: ■ 0.0.0.0 ■ IP from ISP where IP from ISP is the IP address dynamically allocated to you when you connect.
	Phone Line Speed	Speed at which the modem is connected to the ISP. Possible phone line speeds include: ■ Unknown ■ ##### where ##### is a number representing the phone speed. For example, 48800.

PPTP tab field descriptions

The PPTP tab lets you configure the security gateway to connect to the Internet with an account that uses PPTP for authentication.

Table C-16 PPTP tab field descriptions

Section	Field	Description
WAN Port: (Dual WAN port models)	WAN Port (Dual WAN port models)	WAN port for which you are configuring PPTP.

Table C-16 PPTP tab field descriptions (Continued)

Section	Field	Description
Connection	Connect on Demand	When enabled, a connection is established only when a request is made, such as when a user browses to a Web page.
	Idle Time-out	Number of minutes that the connection can remain idle (unused) before disconnecting. Type 0 to keep the connection always on and to prevent the security gateway from disconnecting. For values greater than 0, check Connect on Demand to reconnect automatically when needed.
	Server IP Address	IP address of the PPTP server. The default value for the first octet is 10. The default value for the last octet is 138.
	Static IP Address	Use this field only for static PPTP accounts. Type the static IP address for your account, if you purchased one from, or are assigned one by your ISP.
User Information	User Name	User name for your PPTP account.
	Password	Password for your PPTP account.
	Verify Password	Retype the password for your PPTP account.
Manual Control	Connect	Opens a connection to your PPTP account.
	Disconnect	Closes an open connection to your PPTP account.

Dynamic DNS tab field descriptions

Dynamic DNS services let you use your own domain name (mysite.com, for example) or another domain name and your subdomain to connect to your services, such as a VPN gateway, Web site or FTP. For example, if you set up a virtual Web server and your ISP assigns you a different IP address each time you connect, your users can always access www.mysite.com.

Table C-17 Dynamic DNS tab field descriptions

Section	Field	Description
Service Type	Dynamic DNS Service	Service through which you get your dynamic DNS service. Options include: ■ TZO A dynamic DNS service. ■ Standard There are many standard dynamic DNS services. See the *Symantec Gateway Security 300/400 Series Release Notes* for the list of supported services. ■ Disable The security gateway does not use dynamic DNS.
	WAN Port (Dual WAN port models)	WAN port on which you want to configure dynamic DNS.
	Force DNS Update	Clicking Update sends updated IP information to the dynamic DNS service. Select this field only if requested by Symantec Technical Support.

Table C-17 Dynamic DNS tab field descriptions (Continued)

Section	Field	Description
TZO Dynamic DNS Service	Key	An alphanumeric string of characters that acts as a password for the TZO account. TZO sends the key when the account is created. The maximum TZO key length is 16 characters.
	Email	Email address that acts as a user name with the TZO service.
	Domain	Domain name that you want to manage with the TZO service. For example, marketing.mysite.com.
Standard Service	User Name	User name for the account that you create with a dynamic DNS service.
	Password	Password for the account that you create with a dynamic DNS service.
	Verify Password	Retype the dynamic DNS account password.
	Server	IP address or DNS-resolvable name of the server that provides the dynamic DNS service. For example, members.dyndns.org.
	Host Name	The name to assign to the security gateway. For example, if you want marketing as the host name, and the domain name is mysite.com, you access the security gateway by marketing.mysite.com.
Standard Optional Settings	Wildcards	Enables external access to *.yoursite.yourdomain.com where: ■ * is a CNAME like www, mail, irc, or ftp. ■ yoursite is the host name. ■ yourdomain.com is your domain name.
	Backup MX	Enables a backup mail exchanger. If you check this check box, the mail exchanger you specify in the Mail Exchanger text box is used first; if it fails, the backup mail exchanger (supplied by the dynamic DNS service) takes its place.
	Mail Exchanger	Mail exchangers specify the server that you want to handle email sent to a given domain name. For example, you have two domains, www.mysite.com and mail.mysite.com. Your Web server is configured to allow browsing to both www.mysite.com and mysite.com. You want email that comes to @mysite.com to be handled by the mail server and not the Web server. You set up a mail exchanger to redirect @mysite.com email to mail.mysite.com. Host names in mail exchangers cannot be CNAMEs. You cannot specify your mail exchanger using an IP address. Refer to your dynamic DNS service documentation for more information.

Routing tab field descriptions

Use the routing table to configure static or dynamic routing for your security gateway.

Table C-18 Routing tab field descriptions

Section	Field	Description
Dynamic Routing	Enable RIP v2	Enables dynamic routing. Use this only for intranet or department gateways.

Table C-18 Routing tab field descriptions (Continued)

Section	Field	Description
Static Routes	Route Entry	Select an entry from the list to edit or delete.
	Destination IP	IP address/subnet for traffic requiring routing.
	Netmask	Netmask (used with the destination IP address) to set range of IP addresses for traffic requiring routing.
	Gateway	IP address of the router to which to send traffic that meets the IP address and netmask combination of the destination.
	Interface	The appliance interface to which the defined traffic is routed. The options include: ■ Internal LAN ■ External WAN 1 ■ External WAN 2
	Metric	An integer representing the order in which you want the routing statement executed; for example, 1 is executed first.
Routing Table List	Destination	IP address/subnet for traffic requiring routing.
	Mask	Mask (used with the destination IP address) to set range of IP addresses for traffic requiring routing.
	Gateway	IP address of the router to which to send traffic that meets the IP address and netmask combination of the destination.
	Interface	The appliance interface to which the defined traffic is routed.
	Metric	An integer representing the order in which you want the routing statement executed. For example, 1 is executed first.

Advanced tab field descriptions

Use the Advanced tab to configure optional connection settings and the DNS gateway.

Table C-19 Advanced tab field descriptions

Section	Field	Description
Load Balancing	WAN 1 Load (Dual WAN port models)	Percentage of traffic to pass through WAN 1. The remainder of traffic passes through WAN 2. For example, if you type 80%, WAN 1 passes 80% of the traffic and WAN 2 passes 20%. The default percentage is 50%.
	Bind SMTP with WAN Port (Dual WAN port models)	Determines the WAN port (and subsequently, which ISP) through which email is sent. This is useful if you have two different ISPs configured, one for each WAN port. In this case, outgoing email is sent on the WAN port to which SMTP is bound. Outgoing client mail is sent on the WAN port that the client is using and is therefore sent through the ISP (connection type) that is configured for that port. Options include: ■ None (either) Sends email through either WAN port. ■ WAN1 Binds SMTP to WAN1. ■ WAN2 Binds SMTP to WAN2.
Optional Connection Settings	Idle Renew DHCP	Number of minutes after which, if there is no LAN-to-WAN or WAN-to-LAN traffic, the security gateway sends a request to renew the DHCP lease. To disable this feature, type 0.
	Force Renew (Single WAN port models)	Clicking Force Renew sends a request to the ISP to renew the DHCP lease.
	Renew WAN1, Renew WAN2 (Dual WAN port models)	Clicking Renew WAN1 or Renew WAN2 sends a request to the ISP to renew the DHCP lease for WAN1 or WAN2.
	WAN Port 1 WAN Port 2 (Dual WAN port models)	Maximum size (in bytes) of packets that leave through the WAN port you are configuring. The default value is 1500 bytes. For PPPoE, the default value is 1472 bytes.
PPP Settings	Echo Request Time-out	Number of seconds between echo requests.
	Echo Request Retries	Number of times that the security gateway sends echo requests.
DNS Gateway	DNS Gateway	IP address of a non-ISP (private or internal) DNS gateway to use for name resolution.
	Enable DNS Gateway Backup	If you specify a DNS gateway and it becomes unavailable, this enables the appliance to use your ISP's DNS servers as a backup.

Firewall field descriptions

The Symantec Gateway Security 300/400 Series includes firewall technology that lets you define inbound and outbound rules governing the traffic that passes through the security gateway. When configuring the firewall you need to identify all nodes (computers) that are protected on your network.

This section contains the following topics:

- Computers tab field descriptions
- Computer Groups tab field descriptions
- Inbound Rules field descriptions
- Outbound Rules tab field descriptions
- Services tab field descriptions
- Special Applications tab field descriptions
- Advanced tab field descriptions

Computers tab field descriptions

Before configuring outbound or inbound rules, you must identify all nodes (computers) on the Computers tab.

Table C-20 Computers tab field descriptions

Section	Field	Description
Host Identity	Host	Select a host name (network name) from the list to edit or delete.
	Host Name	Defines the name of the host (a computer on your internal network). Use a short descriptive name. You should use the host name or DNS name in the computer's network properties.
	Adapter (MAC) Address	Physical address of the host's network interface card (NIC), usually an Ethernet or wireless card.
	Computer Group	Displays all of the computer groups to which you can bind hosts. Computer groups let you group computers to which you want to apply the same rules. The options include: ■ Everyone ■ Computer Group 1 ■ Computer Group 2 ■ Computer Group 3 ■ Computer Group 4
Application Server	Reserved Host	Adds the MAC address (that you specified in the Adapter (MAC) Address text box) to the appliance's DHCP server so it is always assigned to the IP address that you specify in the IP Address text box. This is required for application servers. Checking this check box ensures that the DHCP server always offers the defined IP address to the computer you are defining, or you can set this IP address as a static address on the computer.
	IP Address	Defines the IP address of the application server.

Table C-20 Computers tab field descriptions (Continued)

Section	Field	Description
Session Associations - Optional	Bind with WAN port (Dual WAN port models)	Binds this computer to a particular WAN port so that its traffic only goes out through that WAN port. This is useful if you have two broadband accounts configured, one for each WAN port, and you want that computer's traffic to go through only one of the ISPs.
	Bind with PPPoE Session	Displays all of the PPPoE sessions that you can bind to access groups and rules: ■ Session 1 ■ Session 2 ■ Session 3 ■ Session 4 ■ Session 5 Only select a session if your ISP service includes multiple PPPoE sessions.
Host List	Host Name	Name of the host (a computer on your internal network).
	Adapter (MAC) Address	Physical address of the host's network interface card (NIC), usually an Ethernet or wireless card.
	App Server	IP address of the application server.
	Computer Group	Computer group to which the host is assigned.
	PPPoE Session	PPPoE session to which the host is bound.

Computer Groups tab field descriptions

Computer groups help you to group together computers (defined on the Computers tab) so that you can apply inbound and outbound rules.

Table C-21 Computer Groups tab field descriptions

Section	Field	Description
Security Policy	Computer Group	Select a computer group to edit or delete.
Antivirus Policy Enforcement	Enable Antivirus Policy Enforcement	If you enable AVpe for the selected computer group, the security gateway monitors client workstations to determine their compliance with current antivirus software and security policies. For each group, options include: ■ Warn Only (default) A client with non-compliant virus software or virus definitions is still allowed access. A log message warns the administrator that the client is non-compliant. ■ Block Connections A client with non-compliant virus software or virus definitions is denied access to the external network. The client is allowed access to the Symantec Antivirus CE Server or LiveUpdate server to bring their virus definitions into compliance.

Table C-21 Computer Groups tab field descriptions (Continued)

Section	Field	Description
Content Filtering	Enable Content Filtering	If you enable content filtering for the selected computer group, the security gateway allows or blocks access to URLs contained in the Content Filtering allow and deny lists. For each group, options include: ■ Use Deny List A list of blocked URLs, all others are allowed. ■ Use Allow List (default) A list of URLs that permit access to the sites; all other sites are blocked.
Access Control (Outbound Rules)	No restrictions	A host assigned to this group may pass any traffic to the external network. You do not need to define rules for access groups in this category. The No Restrictions setting overrides any outbound rules. This is the default setting.
	Block ALL outbound access	When an access group is configured to block all Internet access behavior, all outbound traffic is blocked. A host assigned to this group may not pass any traffic through the security gateway. No rules need to be defined for access groups in this category. This is useful for computers that only require access to the LAN and do not require access to the external network, for example network printers.
	Use rules defined in Outbound Rules Screen	When an access group is configured to use rules that are defined in the Outbound Rules tab, you must specify the type of traffic that the host, as a member of that logical group, may pass. Do this by creating an outbound rule. When this option is used, hosts are only allowed to pass traffic that matches the outbound rule list for that access group. The outbound default state of the security gateway is that all outbound traffic is blocked until outbound rules are configured to allow certain kinds of outbound traffic.

Inbound Rules field descriptions

The Inbound Rules tab lets you define the type of traffic that can access your internal network.

Table C-22 Inbound Rules fields description

Section	Field	Description
Inbound Rules	Rule	Select an inbound rule to edit or delete.
Rule Definition	Name	Type a new name when adding a rule.
	Enable Rule	Check to enable the inbound rule.
	Application Server	Shows the configured application servers available for inbound rules. These application servers are configured on the Computers tab.
	Service	Type of traffic applied to the rule. It includes both the list of predefined services and any custom services that you have created.
Inbound Rules List	Enabled?	Indicates whether the inbound rule is enabled for use.
	Name	Name of the inbound rule.
	Service	The service that this inbound rule governs, such as HTTP or FTP.

Outbound Rules tab field descriptions

The Outbound Rules tab lets you define the types of traffic that can leave your network to access other networks or the Internet.

Table C-23 Outbound Rules tab field descriptions

Section	Field	Description
Computer Groups	Computer Group	Select a group to edit or add rules for the group.
Outbound Rules	Rule	Select an outbound rule to update or delete.
	Rule Name	Name of the outbound rule.
	Enable Rule	Check to enable the outbound rule.
	Service	The service that the outbound rule governs.
Outbound Rules List	Enabled?	Displays Y or N (Yes or No). Indicates whether the outbound rule is enabled for use.
	Name	Name of the outbound rule.
	Service	The service that the outbound rule governs.

Services tab field descriptions

Define the services to be used in the outbound and inbound firewall rules on the Services tab.

Table C-24 Services tab field descriptions

Section	Field	Description
Services	Application	Select an application for services to edit or delete. Supported applications include: ■ DNS ■ FTP ■ HTTP ■ HTTPS ■ Mail (SMTP) ■ Mail (POP3) ■ RADIUS Auth ■ Telnet ■ VPN IPSec ■ VPN PPTP ■ LiveUpdate ■ SESA Server ■ SESA Agent ■ Real Audio ■ PCA TCP ■ PCA UDP ■ TFTP ■ SNMP

Table C-24 Services tab field descriptions (Continued)

Section	Field	Description
Application Settings	Name	Name of the service you are creating.
	Protocol	Select the protocol associated with the service. Options include: ■ TCP ■ UDP The default depends on the selection you made in the Application drop-down list.
	Listen on Port(s)	Defines the range of ports that listen for packets. ■ Start Type the first port in the range of listen on ports. ■ End Type the last port in the range of listen on ports. The quantity of ports in the range must match the selection made in the Redirect to Port(s) field. For example, if you set the Listen on Port(s) range to 20 to 27, the Redirect to Port(s) range must also be 7 ports. The defaults depend on the selection you made in the Application drop-down list.
	Redirect to Port(s)	Defines the range of ports to which the packets are redirected. ■ Start Type the first port in the range of redirect to ports. ■ End Type the last port in the range of redirect to end ports. The quantity of ports in the range must match the selection made in the Listen on Port(s) field. For example, if you set the Redirect to Port(s) range to 20 to 27, the Listen on Port(s) range must also be 7 ports. The defaults depend on the selection you made in the Application drop-down list.
Service List	Name	Name of the service.
	Protocol	Protocol associated with the service.
	Listen on Start Port	First port in the range on which to listen.
	Listen on End Port	Last port in the range on which to listen.
	Redirect to Start Port	First port in the range to which to redirect.
	Redirect to End Port	Last port in the range to which to redirect.

Special Applications tab field descriptions

Certain applications with two-way communication (games, video or teleconferencing) require dynamic ports on the security gateway. Use the Special Applications tab to define those applications.

Table C-25 Special Applications tab field descriptions

Section	Field	Description
Special Applications	Application	Select a special application to update or delete.

Table C-25 Special Applications tab field descriptions (Continued)

Section	Field	Description
Special Application Settings	Name	Name of the special application.
	Enable	Enables the special application for all computer groups.
	Incoming Protocol	Protocol for the incoming packets. Options include: ■ TCP ■ UDP
	Listen on Port(s)	Range of ports on which the packets are received. ■ Start First port in the range of incoming ports. ■ End Last port in the range of incoming ports.
	Outgoing Protocol	Protocol for outgoing packets. Options include: ■ TCP ■ UDP
	Incoming Port(s)	Range of ports on which the packets are sent. ■ Start First port in the range of outgoing ports. ■ End Last port in the range of outgoing ports.
Special Application List	Name	Name of the special application.
	Enabled	Indicates whether the special application is enabled for all computer groups.
	Incoming Protocol	Protocol for the incoming packets.
	Listen on Start Port	First port in the range of incoming ports.
	Listen on End Port	Last port in the range of incoming ports.
	Outgoing Protocol	Protocol for outgoing packets.
	Redirect to Start Port	First port in the range of ports to which to redirect traffic.
	Redirect to End Port	Last port in the range of ports to which to redirect traffic.

Advanced tab field descriptions

You configure advanced firewall settings, such as IPsec pass-thru, on the Advanced tab.

Table C-26 Advanced tab field descriptions

Section	Field	Description
Optional Security Settings	Enable IDENT Port	Disabling the IDENT port closes port 113; it is not open (in stealth mode). You should enable this setting only if there are problems accessing a server. The IDENT port normally contains the security gateway host name or company name information. By default, the security gateway sets all ports to stealth mode. This makes a computer appear invisible outside of the network. Some servers, such as some email or Microsoft Internet Relay Chat (MIRC) servers, view the IDENT port of the system accessing them.
	Disable NAT Mode	Disabling Network Address Translation (NAT) mode disables the firewall security functions. Only use this setting for intranet security gateway deployments where, for example, the security gateway is used as a bridge on a protected network. When the security gateway is configured for NAT mode, it behaves as an 802.1D bridge device.
	Block ICMP Requests	Clicking Enable blocks Internet Control Message Protocol (ICMP) requests, such as PING and traceroute, to the WAN ports. To allow ICMP requests, click Disable.
	WAN Broadcast Storm Protection	Enabling broadcast storm protection protects regular traffic from an overabundance of broadcast traffic. For example, a condition may exist in which a broadcast message results in many responses, each of which results in still more responses. This filter triggers when 63% of the WAN buffers are taken up by broadcast packets. You may want to disable this feature to allow games that require broadcast packets.
IPsec Passthru Settings	IPsec Type	These values are used in Encapsulation Security Payloads (ESP) IPSec VPNs from some vendors for software clients for IPsec pass-thru compatibility. These settings do not apply to the VPN gateway on the security gateway. Keep this setting at the default 2 SPI (Security Parameter Indices) unless instructed by Symantec Technical Support to change it. The None setting lets VPN clients be used in exposed host mode if they are having problems connecting from behind the security gateway. Options include: ■ 1 SPI ADI (Assured Digital) ■ 2 SPI Normal (Cisco Client, Symantec Client VPN, Nortel Extranet, Checkpoint SecureRemote) ■ 2 SPI-C (Cisco VPN Concentrator 30x0 series (formerly Altiga)) ■ Others Redcreek Ravlin Client ■ None Use only for debugging clients.

Table C-26 Advanced tab field descriptions (Continued)

Section	Field	Description
Exposed Host	Enable Exposed Host	Check to enable an exposed host. Activate this feature only when required. This lets one computer on a LAN have unrestricted two-way communication with Internet servers or users. This feature is useful for hosting games or special server or application.
	LAN IP Address	IP address of the exposed host. If a host is defined as an exposed host, all traffic not specifically permitted by an inbound rule is automatically redirected to the exposed host.
	Bind with WAN Port (Dual WAN port models)	Select the WAN port to bind to the exposed host. The default is WAN port 1.
	Session	In the drop-down list, select the session to bind to the exposed host.

VPN field descriptions

Virtual Private Networks (VPNs) let you securely extend the boundaries of your internal network to use insecure communication channels (such as the Internet) to safely transport sensitive data. VPNs are used to allow a single user or a remote network access to the protected resources of another network.

The Symantec Gateway Security 300/400 Series security gateways support two types of VPN tunnels: Gateway-to-Gateway and Client-to-Gateway.

This section contains the following topics:

- Dynamic Tunnels tab field descriptions
- Static Tunnels tab field descriptions
- Client Tunnels tab field descriptions
- Client Users tab field descriptions
- VPN Policies tab field descriptions
- VPN Status tab field descriptions
- Advanced tab field descriptions

Dynamic Tunnels tab field descriptions

The Dynamic Tunnels tab lets you configure dynamic Gateway-to-Gateway VPN tunnels.

Table C-27 Dynamic Tunnels field descriptions

Section	Field	Description
IPSec Security Association	VPN Tunnel	Select a tunnel to update or delete.
	Name	Name of the tunnel. The tunnel name can be up to 25 alphanumeric characters, dashes, and underscores. This name used only for reference within the SGMI. You can create up to 50 tunnels.
	Enable VPN Tunnel	Enables the tunnel you are defining so it can be used by remote VPN users. To temporarily disable the tunnel, uncheck this check box and click Update. To permanently disable the tunnel, click Delete.
	Phase 1 Type	Select a mode for phase 1 negotiation. Options include: ■ Main Mode Negotiates with a source IP address. ■ Aggressive Mode Negotiates with an identifier such as a name. Client VPN software typically negotiates in aggressive mode. The default value is Main Mode.
	VPN Policy	Select a policy that dictates authentication, encryption, and timeout settings. The list contains Symantec pre-defined policies and any policies you created on the VPN Policies tab.

Table C-27 Dynamic Tunnels field descriptions (Continued)

Section	Field	Description
Local Security Gateway	PPPoE Session	The default PPPoE session is Session 1. This requires an ISP PPPoE account. If you have a single-session PPPoE account, leave the PPPoE session at Session 1.
	Local Endpoint (Dual WAN port models)	Port on the security gateway where you want the tunnel to end. Options include: ■ WAN1 ■ WAN2
	ID Type	ID type used for ISAKMP negotiation. Options include: ■ IP Address ■ Distinguished Name The default value is IP Address.
	Phase 1 ID	The value that corresponds to the ID Type. This value is used to identify the security gateway during phase 1 negotiations. If you selected IP Address, type an IP address. If you selected Distinguished Name, type a fully qualified domain name. If you select IP Address and leave this field blank, the default value is the IP address of the security gateway's internal interface. The maximum value is 31 alphanumeric characters.
	NetBIOS Broadcast	Allows browsing of the VPN network in the Network Neighborhood and file sharing on a Microsoft Windows computer. A Windows Internet Naming Service (WINS) host is needed to accept the traffic. NetBIOS broadcast is disabled by default.
	Global Tunnel	Normally, only requests destined to the network protected by the remote VPN Gateway are forwarded through the VPN. Other traffic, like Web browsing are forwarded straight to the Internet. Enabling Global Tunnel forces all external traffic to the previously-defined VPN Gateway. This lets the Main office's firewall filter traffic before sending the request to the Internet. This provides your remote site with firewall protection from the Main site. Destination Networks should be blank with Global Tunnel enabled. Enabling Global Tunnel also disables all other SAs since all traffic must be routed through the global tunnel gateway. The global tunnel is disabled by default.

Table C-27 Dynamic Tunnels field descriptions (Continued)

Section	Field	Description
Remote Security Gateway	Gateway Address	IP address or fully qualified domain name of the remote gateway (the gateway to which the tunnel will connect). The maximum number of alphanumeric characters for this text box is 128.
	ID Type	ID type used for ISAKMP negotiation. Options include: ■ IP Address ■ Distinguished Name The default value is IP Address.
	Phase 1 ID	The value that corresponds to the ID Type. If you selected IP Address, type an IP address. If you selected Distinguished Name, type a fully qualified domain name. The maximum number of alphanumeric characters in this text box is 31.
	Pre-Shared Key	Key for authenticating ISAKMP (IKE) users. It authenticates the remote end of the tunnel. The pre-shared key is between 20 and 64 alphanumeric characters. The pre-shared key on the remote end of this tunnel must match this value.
	Remote Subnet IP	IP address of the remote subnet.
	Mask	Mask of the remote subnet.

Static Tunnels tab field descriptions

The Static Tunnels tab lets you configure static Gateway-to-Gateway VPN tunnels for the security gateway.

Table C-28 Static Tunnel tab field descriptions

Section	Field	Description
IPSec Security Association	VPN Tunnel	Select a tunnel to update or delete.
	Tunnel Name	Name of the static tunnel. This name is only used for reference within the SGMI. The maximum tunnel name is 50 characters. You can create up to 50 static tunnels.
	Enable VPN Tunnel	Enable the tunnel you are defining so that it can be used by remote VPN users. To temporarily disable the tunnel, uncheck this box, and then click Update. To permanently disable the tunnel, click Delete.
	PPPoE Session	This requires an ISP PPPoE account. The default PPPoE session is Session 1. If you have a single-session PPPoE account, leave the PPPoE session at Session 1.
	Local Endpoint (Dual WAN port models)	The port on the security gateway where you want the tunnel to end.
	Incoming SPI	Incoming security parameter index (SPI) on the IPSec packet. This value must match the outgoing SPI on the remote end of the tunnel. The default value is a decimal number. Prepend the value with 0x for hex numbers. This number between 257 and 8192 identifies the tunnel.
	Outgoing SPI	Outgoing SPI on the IPSec packet. This value must match the incoming SPI on the remote end of the tunnel. The default value is a decimal number. Prepend the value with 0x for hex numbers. This number between 257 and 8192 identifies the tunnel.
	VPN Policy	The policy that dictates authentication, encryption, and timeout settings. This list contains pre-defined policies and any policies you created on the VPN Policies tab.
	Encryption Key	Key for encrypting the data section of the IPsec packet. The key scrambles and de-scrambles your transmitted data. The default number type is decimal. For hex numbers, prepend the value with 0x. Key length depends on the encryption strength specified in the VPN policy. The remote end must have a matching encryption key.
	Authentication Key	Key for authenticating IPsec packets. The default number type is decimal. For hex numbers, prepend this value with 0x. Key length depends on the authentication type (MD5, SHA1, and so on) selected in the VPN policy.

Table C-28 Static Tunnel tab field descriptions (Continued)

Section	Field	Description
Remote Security Gateway	Gateway Address	IP address or fully qualified domain name of the security gateway to which you are creating a tunnel. The maximum length for this field is 128 alphanumeric characters.
	NetBIOS Broadcast	Clicking Enable allows browsing of the VPN network in the Network Neighborhood and file sharing on a Microsoft Windows computer. A WINS host is needed to accept the traffic. NetBIOS is disabled by default.
	Global Tunnel	Normally, only requests destined to the network protected by the remote VPN gateway are forwarded through the VPN. Other traffic, like Web browsing are forwarded straight to the Internet. Enabling Global Tunnel forces all external traffic to the previously-defined VPN gateway. This lets the Main office's firewall filter traffic before sending the request to the Internet. This provides your remote site with firewall protection from the Main site. Destination networks should be blank with Global Tunnel enabled. Enabling Global Tunnel also disables all other SAs since all traffic must be routed through the global tunnel gateway. The global tunnel is disabled by default.
	Remote Subnet IP	IP address of the remote subnet.
	Mask	Mask of the remote subnet.

Client Tunnels tab field descriptions

Use the Client Tunnels tab to define client-to-gateway tunnels. Ensure that you have defined your users on the Client Users tab before defining the tunnel.

Table C-29 Client tunnel tab field descriptions

Section	Field	Description
Group Tunnel Definition	VPN Group	Select a VPN Group to update or delete. You can modify the membership of these three groups. You cannot add VPN groups.
	Enable client VPNs on WAN side	Lets defined VPN users connect to the WAN interface.
	Enable client VPNs on WLAN/LAN side	Lets defined VPN users connect to LAN and wireless LAN interface.
VPN Network Parameters	Primary DNS	IP address of the primary DNS server that resolves names for the VPN user.
	Secondary DNS	IP address of the secondary DNS server that resolves names for the VPN user.
	Primary WINS	IP address of the primary WINS server. Windows Internet Naming Service (WINS) is a system that determines the IP address associated with a particular network computer.
	Secondary WINS	IP address of the secondary WINS server.
	Primary Domain Controller (PDC)	IP address of the Primary Domain Controller (PDC).

Table C-29 Client tunnel tab field descriptions (Continued)

Section	Field	Description
Extended User Authentication	Enable Extended User Authentication	Requires all users in the selected VPN group use RADIUS for extended authentication after phase 1, but before phase 2.
	RADIUS Group Binding	If a RADIUS group binding is specified, the remote user must be a member of that group on the RADIUS Server. The filter ID returned from RADIUS must match this value to authenticate the user. When specifying RADIUS group bindings, no two client tunnels may have the same setting for the group binding. The maximum length of the value is 25 characters.
WAN Client Policy	Enable Content Filtering	Traffic for all clients in the selected VPN group is subject to the content filtering rules defined in allow and deny lists.
	Use Deny List	Content filtering uses the deny list, a list of URLs that clients are not permitted to view, allowing all other traffic.
	Use Allow List	Content filtering uses the allow list, a list of URLs that clients are permitted to view, blocking all other traffic. This is the default.
	Enable Antivirus Policy Enforcement	Requires all users in the selected VPN group to have Symantec antivirus software updated with the most current virus definitions.
	Warn Only	A client with non-compliant antivirus software or virus definitions is still allowed access. A log message warns the administrator that the client is non-compliant.
	Block Connections	A client with non-compliant antivirus software or virus definitions is denied access to the external network. The client is allowed access to the Symantec Antivirus CE Server or LiveUpdate server to bring their virus definitions into compliance.

Client Users tab field descriptions

Use the Client Users tab to define the remote users that are permitted to access your network through a VPN tunnel.

Table C-30 Client Users tab field descriptions

Section	Field	Description
VPN User Identity	User	Select a user to update or delete.
	Enable	Enables a VPN tunnel for the specified user. To temporarily suspend a user, uncheck Enable, and then click Update. To permanently remove a user, click Delete.
	User Name	User name for the client user. The maximum number of alphanumeric characters for this value is 31. It must match the remote Client ID in Symantec Client VPN software. You can add up to 50 client users.
	Pre-Shared Key	ISAKMP (IKE) authenticating key. The key is unique to this user. You must enter a pre-shared key. The maximum number of alphanumeric characters for this value is 64. The pre-shared key must match the pre-shared key offered by the remote VPN client.
	VPN Group	Defines the VPN Group (tunnel definition) for this user.

VPN Policies tab field descriptions

You select one VPN policy for each tunnel. Use the VPN Policies tab to define each policy, or to edit a default policy.

Table C-31 VPN policies field descriptions

Section	Field	Description
IPsec Security Association (Phase 2) Parameters	VPN Policy	Select a policy to update or delete. You cannot delete Symantec pre-defined policies. Options include: ■ ike_default_crypto ■ ike_default_crypto_strong ■ Static_default_crypto ■ Static_default_crypto_strong ■ Any VPN policies you created
	Name	Name to assign to the policy. This name is used for SGMI reference only. The maximum value is 28 alphanumeric characters.
	Data Integrity (Authentication)	Options include: ■ ESP MD5 (default) ■ ESP SHA1 ■ AH MD5 ■ AH SHA1 This selection must match the remote security gateway. When ESP is used, the specified data integrity algorithm is applied only to the data portion of the tunnel packets. ESP provides integrity, authentication, and confidentiality to the packet. It works between hosts, between the host and the security gateway, or between security gateways, ensuring that data has not been modified in transit. If you do not want to use the ESP default, you can elect to use only AH. AH provides integrity and authentication to the entire IP datagram packet. It holds authentication information by computing a cryptographic function for the packets using a secret authentication key. When using AH, a Data Confidentiality selection is optional. If you use AH in your VPN policy and also use a Data Confidentiality Algorithm, ESP is applied to the packets as well as AH.
	Data Confidentiality (Encryption)	Options include: ■ DES ■ 3DES ■ AES_VERY_STRONG (256-bit keys) ■ AES_STRONG (192-bit keys) ■ AES (128-bit keys) ■ NULL (none) The Data Confidentiality Algorithm determines the type of encryption method to be used for tunnel data. If you have selected an AH Data Integrity Authentication, you do not need to select an encryption type. The AES options are not supported for IKE.
	SA Lifetime	Time, in minutes, before phase 2 renegotiation of new encryption and authentication keys for the tunnel. The default value is 480 minutes (8 hours). The maximum value is 2,147,483,647 minutes.

Table C-31 VPN policies field descriptions (Continued)

Section	Field	Description
	Data Volume Limit	Maximum number of kilobytes allowed through a tunnel before a rekey is required. The default value is 2100000 KB (2050 MB). The maximum value is 4200000 KB (4101 MB).
	Inactivity Time-out	Number of minutes a tunnel can be inactive before it is terminated. Type 0 for no timeout (tunnel remains active).
	Perfect Forward Secrecy	Perfect Forward Secrecy (PFS) provides additional protection from attackers trying to guess the current ISAKMP key by using Diffie-Hellman to establish a shared secret. When the tunnel mode is Main Mode, the Diffie-Hellman group is based on what both sides negotiated during Phase 1. In Aggressive Mode, the Diffie-Hellman group is always Group 2. Not all clients and security gateways are compatible with PFS. Options include: ■ DH Group 1 (768 bits long) ■ DH Group 2 (1024 bits long) ■ DH Group 5 (1536 bits long)

VPN Status tab field descriptions

The Status tab shows the status of your VPN tunnels and client users.

Table C-32 Status tab field descriptions

Section	Field	Description
Dynamic VPN Tunnels	Status	Status of the selected tunnel.
	Name	Name of the selected tunnel.
	Negotiation Type	Configured negotiation type. This field applies to dynamic VPN tunnels only.
	Security Gateway	Name of the selected security gateway.
	Remote Subnet	Address of the remote subnet.
	Encryption Method	Configured encryption method.
Static VPN Tunnels	Status	Displays connected or disconnected.
	Name	Name of the selected static tunnel.
	Security Gateway	IP address of the remote gateway to which the tunnel is connected.
	Remote Subnet	Subnet of the remote gateway to which the tunnel is connected.
	Encryption Method	Authentication method for this tunnel.

Advanced tab field descriptions

The Advanced tab lets you configure advanced VPN settings for phase 1 negotiation, which apply to all clients.

Table C-33 Advanced tab field descriptions

Section	Field	Description
Global VPN Client Settings	Local Gateway Phase 1 ID Type	Phase 1 ID (ISAKMP) used by the local gateway for VPN clients. Options include: ■ IP Address If you select IP Address, leave the Local Gateway Phase 1 ID text box blank. ■ Distinguished Name If you select Distinguished Name, in the Local Gateway Phase 1 ID text box, type a local gateway Phase 1 ID to be used by all clients.
	Local Gateway Phase 1 ID	Value that corresponds to the ID Type. If you selected IP address, leave this text box blank. If you selected Distinguished Name, type a fully qualified domain name. Any client connected to the security gateway must use this Phase 1 ID when defining a remote gateway endpoint on the client. The maximum value is 31 alphanumeric characters.
	VPN Policy	VPN policy for VPN client tunnels for phase 2 tunnel negotiation. The list shows pre-defined Symantec policies and any policies you created on the VPN Policies tab.
Dynamic VPN Client Settings	Enable Dynamic VPN Client Tunnels	Lets undefined VPN clients connect to the security gateway for extended authentication.
	Pre-shared Key	Key for authenticating ISAKMP (IKE). It authenticates the remote end of the tunnel. The pre-shared key is between 20 and 64 alphanumeric characters. The pre-shared key on the remote end of this tunnel must match this value.
Global IKE Settings (Phase 1 Rekey)	SA Lifetime	Time, in minutes, before phase 1 renegotiation of new encryption and authentication keys for the tunnel. The default value is 1080 minutes. The maximum value is 2,147,483,647 minutes.
RADIUS Settings	Primary RADIUS Server	IP address or fully qualified domain name of the server used to process extended authentication exchanges with VPN clients. The maximum values is 128 alphanumeric characters.
	Secondary RADIUS Server	IP address or fully qualified domain name of the alternate server used to process extended authentication exchanges with VPN clients. The maximum values is 128 alphanumeric characters.
	Authentication Port (UDP)	Port on the RADIUS server used for authentication. The default value is 1812. The maximum value is 65535.
	Shared Secret or Key	Authentication key used between the RADIUS server and the appliance. The maximum value is 50 alphanumeric characters.

IDS/IPS field descriptions

The Symantec Gateway Security 300/400 Series provides intrusion detection and intrusion prevention (IDS/IPS). The IDS/IPS functions are enabled by default, and provide atomic packet protection with spoof protection and IP. You may disable IDS/IPS functionality at any time.

The following types of protection are offered with the IDS/IPS feature:

- IP spoofing protection
- IP options verification
- TCP flag validation
- Trojan horse protection
- Port scan detection

This section contains the following topics:

- IDS Protection tab field descriptions
- Advanced tab field descriptions

IDS Protection tab field descriptions

Configure basic IDS protection on the IDS Protection tab.

Table C-34 IDS Protection tab field descriptions

Section	Field	Description
IDS Signatures	Name	Select a signature to update from the following: ■ *Back Orifice ■ Bonk ■ Fawx ■ *Girlfriend ■ Jolt ■ Land ■ Nestea ■ Newtear ■ Overdrop ■ Ping of Death ■ *Portal of Doom ■ *SubSeven ■ Syndrop ■ Teardrop ■ Winnuke * Asterisk indicates Trojan port detection. Block and Warn is disabled if traffic is explicitly allowed in Inbound Rules.
Protection Settings	Block and Warn	If an attack is detected, blocks the traffic and logs a message.
	Block/Don't Warn	If an attack is detected, blocks the traffic without a logging a message.
	WAN	Enables WAN protection.
	WLAN/LAN	Enables wireless LAN and LAN protection.

Table C-34 IDS Protection tab field descriptions (Continued)

Section	Field	Description
Protection List	Attack Name	Name of the IDS signatures.
	Block and Warn	Displays Y for yes or N for no. Indicates if the Block and Warn protection setting is enabled for this signature.
	Block/Don't Warn	Displays Y for yes or N for no. Indicates if the Block/Don't Warn protection setting is enabled for this signature.
	WAN	Displays Y for yes or N for no. Indicates if the WAN is protected.
	WLAN/LAN	Displays Y for yes or N for no. Indicates if the wireless LAN and LAN is protected.

Advanced tab field descriptions

You can configure spoof protection on the Advanced tab.

Table C-35 Advanced tab field descriptions

Section	Field	Description
IP Spoof Protection	WAN	Enables spoof protection on the LAN.
	WLAN/LAN	Enables spoof protection on the wireless LAN and LAN.
TCP Flag Validation	TCP Flag Validation	Blocks and logs any traffic with illegal flag combinations for traffic that is not being denied by the security policy. Any traffic denied by the security policy that has one or more bad TCP flag combinations is classified as one of several Network Mapper (NMAP) port scanning techniques (NMAP Null Scan, NMAP Christmas Scan, and so on).

Antivirus Policy field descriptions

The AVpe feature lets you monitor client AVpe configurations and, if necessary, enforce security policies to restrict network access to only those clients who are protected by antivirus software with the most current virus definitions.

Table C-36 AVpe tab field descriptions

Section	Field	Description
Master Location	Primary AV Master	Defines the primary antivirus server in your network. This is the server to which you want the security gateway to connect to verify client virus definitions.
	Secondary AV Master	Defines a secondary antivirus server. The security gateway connects to this server to verify client virus definitions if it cannot access the primary antivirus server.
	Query AV Master Every	Type an interval (in minutes) for the security gateway to query the antivirus server. For example, if you type 10 minutes, the security gateway queries the antivirus server every 10 minutes to obtain the latest virus definition list. The default setting is 10 minutes. You must enter a value greater than 0.
	Query Master	This button lets you override the time interval set in the Query AV Server Every field. When clicked, the security gateway queries the antivirus server for the latest virus definitions. Before you click this button, enter the primary and secondary AV master IP addresses, and then click Save. When first enabling AVpe, use this button to force the security gateway to connect to the primary or secondary antivirus server to obtain current virus definitions.
Policy Validation	Verify AV Client is Active	When enabled, this field lets you verify that Symantec antivirus software is installed and active on a client's workstation. Options include: ■ Latest Product Engine (default) Verifies that Symantec antivirus software is active and that it contains the latest product scan engine. ■ Any Version Verifies that Symantec antivirus software is active with any qualified version of the product scan engine. **Note:** Make sure UDP/Port 2967 is allowed by personal firewalls.
	Verify Latest Virus Definitions	Lets you verify whether the latest virus definitions are installed on a client's workstation before allowing network access. This check box is checked by default.
	Query Clients Every	Type an interval (in minutes) for the security gateway to query client workstations to verify virus definitions. For example, if you type 10 minutes, the security gateway queries the client workstations every 10 minutes to verify that their workstations have the latest virus definitions applied. The default setting is 480 minutes (8 hours).

Table C-36 AVpe tab field descriptions (Continued)

Section	Field	Description
AV Master Status	AV Master	Identifies the antivirus server (either primary or secondary) for which summary information is displayed.
	Status	Indicates the operational status of the antivirus server. Up is displayed when the server is online and functional; Down is displayed when the server is offline.
	Last Update	Displays the date (numerically) when the security gateway last queried the server for virus definition files, for example: 5/14/2003.
	Host	Displays the IP address (or qualified domain name) of the primary or secondary antivirus server.
	Product	Displays the current product version of the Symantec AntiVirus Corporate Edition that the antivirus server is running, for example: 7.61.928.
	Engine	Displays the current version of the Symantec AntiVirus Corporate Edition scan engine that is running on the antivirus server, for example: NAV 4.1.0.15.
	Pattern	Displays the latest version of the virus definition file on the antivirus server, for example: 155c08 r6 (5/14/2003).
AV Client Status	AV Client	IP address of DHCP clients.
	Policy	Displays On or Off. Indicates whether the client has antivirus policies enforced.
	Status	Indicates whether the client is compliant.
	Group	Computer group to which the client is assigned.
	Last Update	Date and time when the client's antivirus compliance was last checked.
	Product	Name of the Symantec antivirus product that the client is using.
	Engine	Version of the scan engine in the Symantec antivirus product that the client is using.
	Pattern	Version of the client's most recent virus definitions.

Content Filtering field descriptions

The security gateway supports basic content filtering for outbound traffic. You use content filtering to restrict the content to which clients have access. For example, to restrict your users from seeing gambling Web sites, you configure content filtering to deny access to the gambling URLs that you specify.

Table C-37 Content filtering configuration fields

Section	Field	Description
Select List	List Type	The possible list types include: ■ Deny (default) ■ Allow A deny list specifies content that you do not want your clients to view. An allow list specifies the content that you permit your clients to view. Select a list, and then click View/Edit.

Table C-37 Content filtering configuration fields (Continued)

Section	Field	Description
Modify List	Input URL	Type a URL to add to the deny or allow list and then click Add. For example, www.symantec.com or myadultsite.com/mypics/me.html. The maximum length of a URL is 128 characters. Each filtering list can hold up to 100 entries. You add URLs one at a time. You must use a fully qualified domain name. Content filtering cannot be performed using an IP address.
	Delete URL	In the drop-down list, select a URL that you want to delete, and then click Delete Entry.
Current List	URL	Depending on the list that you selected, shows all the URLs entered for that list.

Appendix D

Joining security gateways to SESA

This chapter includes the following topics:

- About joining SESA
- Preparing to join SESA
- Trusted certificates
- Joining Symantec Gateway Security 400 Series to SESA
- Logging on to the Symantec Management Console
- Troubleshooting problems when joining SESA
- Leaving SESA

About joining SESA

To join SESA, you use the Advanced Management tab in the Administration area of the Security Gateway Management Interface (SGMI). As the local administrator, you must also have administrative privileges on the SESA Manager to join SESA.

Note: Your SESA environment must be installed and fully operational before installing the Symantec Event Manager and Advanced Manager for Security Gateways (Group 2) v2.1. See the *Symantec Enterprise Security Architecture Installation Guide* for further information.

Joining SESA performs the following tasks:

- Registers the SESA Agent (preloaded on the Symantec Gateway Security 400 Series) with the SESA Manager.
- Downloads configuration settings associated with an organizational unit if you select one.
- Downloads configuration settings associated with the default organizational unit if you do not select a specific organizational unit to join.
- Instructs the SESA Manager to assign the validated configuration with the local security gateway.

Instructions for joining SESA are also provided in the following documentation:

- *Symantec Event Manager and Advanced Manager for Security Gateways (Group 2) v2.1 Administrator's Guide*
- *Symantec Event Manager and Advanced Manager for Security Gateways (Group 2) v2.1 Integration Guide*

They are mirrored here so that SESA administrators can assist you in joining SESA.

Preparing to join SESA

Before you join a security gateway to SESA, you must ensure that the required software is installed and configured.

- On the SESA Manager, install the Symantec Advanced Manager (for both configuration management and event management) and the Symantec Event Manager (for event management only).
- Ensure that the security gateways that you want to manage or from which you want to collect events are installed.
- Configure your security gateway.
  At a minimum, you must run the Setup Wizard to complete the initial setup of your WAN connectivity.
- Back up your local configuration.
  See "Backing up and restoring configurations" on page 103.

Trusted certificates

Note: If you are planning to join SESA using self-signed certificates (the default), you can skip to See "Joining Symantec Gateway Security 400 Series to SESA" on page 161. If you plan to use certificates signed by someone else, you must perform the following procedures.

SESA integration requires Public Key Infrastructure (PKI) services. SESA requires X.509 v3 certificate validation as part of the SSL transport mechanism. SSL provides data integrity and data confidentiality of SESA traffic.

By default, the SESA Manager runs with a self-signed anonymous certificate. You can configure SESA to use a certificate signed by a Certificate Authority (CA). See the *Symantec Event Manager and Advanced Manager for Security Gateways (Group 2) v2.1 Administrator's Guide* for details.

When SESA is using self-signed anonymous certificates, the certificate does not need to be imported to the appliance prior to joining SESA. During the Join SESA operation, the SSL connection downloads the SESA certificate from the SESA Manager to the appliance. Anonymous certificates are valid for one year, after which a new certificate must be imported.

If your environment requires a certificate other than what is provided, Symantec Gateway Security 400 Series includes a PKI module that lets you load different trusted certificates into the appliance. You can import PKCS#7 standard certificates into the appliance and then view the contents of the trusted certificate. If a certificate expires, the PKI module informs the SESA agent for proper logging.

You can load up to three certificates. At least one trusted CA certificate is required for each primary or secondary SESA Manager. The third certificate is used for signing LiveUpdate firmware packages. You can also import the CA root certificate, which eliminates the need to import a new server certificate each year.

Note: If the same CA issues both SESA Manager certificates, you can validate both the primary and secondary SESA Manager SSL server certificates with a single CA certificate.

When SESA is using certificates signed by a CA, you must import the CA root certificate onto the appliance prior to joining SESA. During the join SESA operation, the SSL connection downloads the SESA certificate from the SESA Manager to the appliance.

To install a certificate on the appliance

See "Trusted Certificates tab field descriptions" on page 123.

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the Trusted Certificate tab, click **Browse**.

3 Browse to the location of the certificate authority from which you want to import a certificate.

4 Click **Import**.

To view the contents of a certificate

1 In the SGMI, in the left pane, click **Administration**.

2 In the right pane, on the Trusted Certificates tab, in the Certificate Issued To list, select the certificate you want to view.

3 Click **View**.

To delete a certificate

1 In the SGMI, in the left pane, click **Administration**.

2 In the right pane, on the Trusted Certificates tab, in the Certificate Issued To list, select the certificate you want to delete.

3 Click **Delete**.

Joining Symantec Gateway Security 400 Series to SESA

Joining SESA lets you manage your security gateways from the Symantec management console.

Before you join SESA:

- Determine the join SESA option that you will use.
- For all options, contact your SESA administrator for the following information, which you will need to join SESA:
  - SESA Manager IP address or fully qualified domain name
  - SESA logon name
  - SESA password

Determining your options for joining SESA

For Symantec Gateway Security 400 Series appliances, there are two options for joining a security gateway to SESA. The option that you use depends on the selection you make from the Centralized Management area of the Advanced Management tab in the SGMI.

Table D-1 Options for joining SESA

Type of SESA management	Security gateway configuration option	Description
Centralized Monitoring and Policy Management	Use default organizational unit configuration	When you join a security gateway to SESA, this option automatically associates the default organizational unit with the security gateway.
	Use selected organizational unit configuration	This option lets you select an organizational unit and import the configuration that is associated with it to the local security gateway. This overwrites parts of the configuration on the local security gateway. To use this option, your network resources must be parallel to those defined in the configuration you will import.

Table D-1 Options for joining SESA (Continued)

Type of SESA management	Security gateway configuration option	Description
Centralized Monitoring (Alerting, Logging, and Reporting)	Not applicable. When you join SESA for event management only, you cannot configure the security gateway from SESA.	This option lets you join security gateways to SESA for event management. You use the Symantec Management Console to view the events, and create alerts and reports.

Joining SESA

You can join a security gateway to SESA in one of the following ways:

- Join SESA and use the default organizational unit.
  If you are new to using SESA to manage security gateways, this is the simplest way to connect a security gateway on the SESA Manager. It requires the least amount of preparation on the SESA Manager.
- Join SESA and use a configuration that is associated with a specific organizational unit.
- Join a security gateway to SESA for the purpose of logging and reporting events only.

To join SESA

Use one of the following procedures to join Symantec Gateway Security 400 Series appliances to SESA.

To join the local security gateway to SESA using the default organizational unit

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the Advanced Management tab, under Centralized Management, click **Centralized Monitoring and Policy Management**.
3. Under Symantec Enterprise Security Architecture (SESA) Registration, do the following:

Management Server	Type the IP address or the fully-qualified domain name of the SESA server.
Administrator	Type the SESA administrator logon name.
Password	Type the SESA administrator logon password.

4. Click **Join SESA**.

To join the security gateway to SESA using a specific organizational unit

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the Advanced Management tab, under Centralized Management, click **Centralized Monitoring and Policy Management**.
3. Under Symantec Enterprise Security Architecture (SESA) Registration, do the following:

Query SESA	Click this button to populate the Organizational Unit drop-down list.
Management Server	Type the IP address or the fully-qualified domain name of the SESA server.
Administrator	Type the SESA administrator logon name.
Password	Type the SESA administrator logon password.

Organizational Unit	To join SESA as a member of a specific organizational unit, select the org unit from the **Organizational Unit** drop-down menu. You must click **Query SESA** first to populate this drop-down list.

4 Click **Join SESA**.

To join the security gateway to SESA for event management only

1 In the SGMI, in the left pane, click **Administration**.

2 In the right pane, on the Advanced Management tab, under Centralized management, click **Centralized Monitoring (Alerting, Logging, and Reporting)**.

3 Under Symantec Enterprise Security Architecture (SESA) Registration, do the following:

Management Server	Type the IP address or the fully-qualified domain name of the SESA server.
Administrator	Type the SESA administrator logon name.
Password	Type the SESA administrator logon password.

4 Click **Join SESA**.

Viewing SESA Agent status

At the bottom of the Advanced Management tab, you can view the status of the SESA Agent, including whether or not SESA is enabled,

To view SESA agent status

1 In the SGMI, in the left pane, click **Administration**.

2 On the Advanced Management tab, under Local SESA Agent Status, you can view the following information:

SESA Enabled?	This displays Y when SESA Server is available; N when it is not.
Mode	This displays the management mode, either Management (for full SESA management) or Monitoring (for event logging and reporting only).
Primary Server	This displays the IP address of the primary SESA server.
Secondary Server	This displays the IP address of the secondary SESA server.
SESA ID	This displays the SESA ID of the security gateway SESA Agent.
Status	Status of the local SESA Agent. This can be: ■ Active ■ Activating ■ Deactivating ■ Deactivated

3 To refresh the SESA Agent status display, click **Refresh**.

Understanding how security gateways obtain configurations from SESA

After your security gateway joins SESA, you can obtain configuration information from the SESA Manager in a number of different ways. Running the join SESA procedure provides your security gateway with the configuration associated with either the default organizational unit or the specific organizational unit you requested during the join operation. Once you have joined SESA, the SESA Manager automatically sends out configuration information at a predefined interval to ensure that all security gateways being managed have the same configuration. The SESA Manager also updates all security gateways when the configuration they are using is changed. You can also request a configuration from SESA at any time without waiting for the automatic update.

To obtain a configuration from SESA

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the Advanced Management tab, click **Get Configuration**.

Logging on to the Symantec Management Console

Once your security gateway joins SESA, you log on to the Symantec Management Console to begin managing the security gateway.

To log on to the Symantec management console

1. On your local security gateway system, or on the SESA Manager, open a browser window.
2. Browse to **https://<SESA manager IP address or domain name>/sesa/ssmc**
   where <SESA manager IP address or domain name> is the IP address or fully qualified domain name of your SESA manager.
3. In the Logon name text box, type the SESA administrator's user name.
4. In the Password text box, type the SESA administrator's password.
5. Click **Log On**.

Troubleshooting problems when joining SESA

If the Join SESA procedure fails, verify the following:

- Your information for connecting to SESA is correct:
  - IP address or domain name for the SESA Manager
  - SESA administrator user name and password
- If you are using a specific organizational unit, ensure that the configuration of your local security gateway is consistent with the configuration associated with that organizational unit.
  The network topology of your local security gateway must be parallel to the network topology that is represented by the organizational unit.
  When there is disparity, you can view the validation report in SESA to identify adjustments you must make so that the configuration works correctly with your security gateway.

Leaving SESA

You must manage some aspects of security gateways locally. These include:

- Changing system settings such as network interfaces
- Backing up your security gateway

To make these local changes, you must return the security gateway to local management.

Returning to local management

In the SGMI, two buttons on the Advanced Management tab let you return to local management of your security gateway. Another button lets you return to managing your security gateways from SESA.

Table D-2 Options to return to local security gateway management

Option to manage locally	Reason to use	Option to return to SESA management
Disconnect SESA	Temporarily return to local management to make local changes.	Reconnect SESA
Leave SESA	Permanently remove the registration of the security gateway from SESA.	Join SESA

To return to local management temporarily

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the Advanced Management tab, under Symantec Enterprise Security Architecture (SESA) Registration, click **Disconnect SESA**.
   The security gateway temporarily leaves SESA and you can perform management functions from the local SGMI.

To return to SESA management after leaving temporarily

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the Advanced Management tab, under Symantec Enterprise Security Architecture (SESA) Registration, click **Reconnect SESA**.
   When you reconnect to SESA, the security gateway reestablishes its previous connection to SESA.

To return to local management permanently

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the Advanced Management tab, under Symantec Enterprise Security Architecture (SESA) Registration, click **Leave SESA**.
   If you want to return to SESA management after clicking Leave SESA, you must complete the Join SESA procedure again. See "Joining SESA" on page 162.

Glossary

action	A predefined response to an event or alert by a system or application.
activation	The process of making a configuration available for download and notifying all associated security gateways that it is there. Successful validation is a required piece of the activation process.
active	A status that indicates that a program, job, policy, or scan is running. For example, when a scheduled scan executes, it is considered active. Active is also used to describe the current state of a connection. An active session refers to an existing connection.
address transforms	A process that lets you present routable addresses to the security gateway for packets passing through a security gateway interface or secure tunnel.
administrator	1. A person who oversees the operation of a network. 2. A person who is responsible for installing appliances on a network and configuring them. The administrator may also update security settings on workstations.
aggressive mode	A shortened ISAKMP (IKE) negotiation typically used for clients connecting to gateways where their originating IP address is unknown. Aggressive mode is less secure than the longer main mode, which uses the IP source address as part of the authentication exchange. See also IKE, main mode.
alert	An event or set of events that an administrator should review and potentially configure a notification for. Alerts are used to escalate a single event or a group of events and to draw more attention to the events.
alert threshold	A setting on a rule that instructs the security gateway to monitor suspicious activity based on access attempts and time intervals. You can customize or disable the default threshold according to your needs.
alive indicator	An external (WAN-side) network node that is used as a beacon point to determine if the network connection is operational. If the alive indicator fails, the appliance starts a failover sequence, using DNS requests, to a backup connection.
allow list	Also called a “white list.” A list of URLs that a group of users is allowed to see. Other sites are blocked. This is useful for companies with employees that only need access to a set number of Web sites to perform their tasks.
antivirus	A subcategory of a security policy that pertains to computer viruses. See also antivirus policy enforcement.
application	See integrating product.
application server	A server that lets clients use applications and databases that are managed by the server. You define each application server for use in inbound or outbound rules.
ARP (Address Resolution Protocol)	A protocol for mapping an Internet Protocol (IP) address to a physical computer address, also known as a a MAC address, that is recognized in the local network. When an interface on one computer needs to talk to another interface, it will ARP (that is, send out a broadcast) asking for a response from the interface that matches the IP address. The response contains the hardware address of the interface that has the corresponding IP address.
asynchronous transmission	A form of data transmission in which information is sent intermittently. The sending device transmits a start bit and stop bit to indicate the beginning and end of a piece of data.
attack signature	The features of network traffic, either in the heading of a packet or in the pattern of a group of packets, that distinguish attacks from legitimate traffic.
authentication	The process of determining the identity of a user attempting to access a network. Authentication occurs through challenge/response, time-based code sequences, or other techniques. Authentication typically involves the use of a password, certificate, PIN, or other information that can be used to validate identity over a computer network. See also RADIUS.

bandwidth	The amount of data transmitted or received per unit time. In digital systems, bandwidth is proportional to the data speed in bits per second (bps). Thus, a modem that works at 57,600 bps has twice the bandwidth of a modem that works at 28,800 bps. See also bps.
blended threat	An attack that uses multiple methods to transmit and spread. The damage caused by blended threats can be rapid and widespread. Protection from blended threats requires multiple layers of defense and response mechanisms.
bps (bits per second)	A measure of the speed at which a device such as a modem can transfer bits of data.
broadcast	To simultaneously send the same message to all users on a network.
broadcast storm	A network condition in which broadcast Ethernet or IP packets multiply through switches and cause congestion. Symantec Gateway Security 400 Series appliances offer broadcast storm protection to prevent the condition from affecting normal network traffic.
buffer overflow attack	An attack that exploits a known bug in one of the applications running on a server. This then causes the application to overlay system areas, such as the system stack, thus allowing the attacker to gain administrative rights. In most cases, this gives the attacker complete control over the system. Also called stack overflow.
cable	A group of wires that are enclosed in a protective tube. Usually this is an organized set of wires that correspond to specific pins on a 9- or 25-pin connector located at each end. A cable is used to connect peripheral devices to each other or to another computer. In remote computing, this can refer to a cable that is used to connect a computer to a modem, or a cable that connects two computers directly, which is sometimes called a null modem cable.
client	A requesting program or user in a client/server relationship. For example, the user of a Web browser is effectively making client requests for pages from servers all over the Web. The browser itself is a client in its relationship with the computer that is getting and returning the requested HTML file.
client computer	A computer that is running a client program. In a network, the client computer interacts in a client/server relationship with another computer that is running a server program.
communications	The transfer of data between computers by means of a device such as a modem or cable.
communications device	A modem, network interface card, or other hardware component that enables remote communications and data transfer between computers. Also called connection device.
communications session	The time during which two computers maintain a connection and, usually, are engaged in transferring information.
computer	A defined entity on the LAN or WLAN that firewall rules and security policies are applied to. Not necessarily a PC, a computer can be any Ethernet-enabled device like a printer or scanner. See also computer group.
computer group	A group of LAN or WLAN Ethernet devices that firewall rules and security policies are applied to. For example, all local printers may be in a computer group that has all outbound Internet communication blocked. See also computer.
configuration	A collection of settings that a software feature uses.
content filtering	The use of content-based filters that are applied to traffic passing through a security gateway. You can filter content based on protocol type, subject matter, MIME types, URLs, and filename extensions.
data rate	The speed at which information is moved from one location to another. Data rates are commonly measured in kilobits (thousand bits), megabits (million bits), and megabytes (million bytes) per second. Modems, for example, are generally measured in kilobits per second (Kbps). See also bandwidth, bps.
data transfer	The movement of information from one location to another. The transfer speed is called the data rate or data transfer rate.
data transmission	The electronic transfer of information from a sending device to a receiving device.
data-driven attack	A form of intrusion in which the attack is encoded in seemingly innocuous data. It is subsequently executed by a user or other software to actually implement the attack.
denial of service (DoS) attack	A type of attack in which a user or program takes up all of the system resources by launching a multitude of requests, leaving no resources and thereby denying service to other users. Typically, denial of service attacks are aimed at bandwidth control.

DES (Data Encryption Standard)	A widely-used method of data encryption using a private (secret) key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.
DHCP (Dynamic Host Configuration Protocol)	A method of automatically serving IP addresses and other network settings to receiving hosts that contain a DHCP client. This eliminates having to manually assign IP addresses and other settings to hosts on a network. Most modern OSs have a DHCP client.
dial	To initiate a connection using a LAN, modem, or direct connection, regardless of whether actual dialing is involved.
Diffie-Hellman (DH)	A cryptographic technique that enables sending and receiving parties to exchange public keys in a manner that derives a shared, secret key at both ends. Different strengths are available and are referred to as Group 1, Group 2, and Group 5 (and higher). DH is used as part of VPN negotiations to create new keys. See also Perfect Forward Secrecy.
disabled	A status that indicates that a program, job, policy, or scan is not available. For example, if scheduled scans are disabled, a scheduled scan does not execute when the date and time specified for the scan is reached.
DNS (Domain Name System)	A hierarchical system of host naming that groups TCP/IP hosts into categories. For example, in the Internet naming scheme, names with .com extensions identify hosts in commercial businesses. See also DNS server.
DNS server	A repository of addressing information for specific Internet hosts. Name servers use the Domain Name System (DNS) to map IP addresses to Internet hosts. See also DNS.
domain	A group of computers or devices that share a common directory database and are administered as a unit. On the Internet, domains organize network addresses into hierarchical subsets. For example, the .com domain identifies host systems that are used for commercial business.
domain entity	A group of computers sharing the network portion of their host names, for example, symantec.com. Domain entities are registered within the Internet community. Registered domain entities end with an extension such as .com, .edu, or .gov or a country code such as .jp (Japan).
download	To transfer data from one computer to another, usually over a modem or network. Usually refers to the act of transferring a file from the Internet, a bulletin board system (BBS), or an online service to one's own computer. See also upload.
dynamic DNS	The ability to automatically update a DNS server when an IP address is automatically assigned or changed (typically from an ISP using DSL or cable) to a network gateway. Whenever an assigned IP address changes, the domain name (www.mybranchoffice.com for example) is immediately updated by the gateway to the new IP address. This enables lower-cost dynamic IP Internet accounts for services like VPN or server hosting where static IP accounts are either unavailable or cost-prohibitive.
email server	An application that controls the distribution and storage of email messages.
enabled	A status that indicates that a program, job, policy, or scan is available. For example, if scheduled scans are enabled, any scheduled scan will execute when the date and time specified for the scan is reached.
encryption	A method of scrambling or encoding data to prevent unauthorized users from reading or tampering with the data. Only those who have access to a password or key can decrypt and use the data. The data can include messages, files, folders, or disks.
Ethernet	A local area network (LAN) protocol developed by Xerox Corporation in cooperation with DEC and Intel in 1976. Ethernet uses a bus or star topology and supports data transfer rates of 100 Mbps.
event	A message that is generated by a product to indicate that something has happened.
event class	A predefined event category that is used for sorting reports and configuring alerts.
Event Collector	An application that collects events from security products, processes them, and places them in the SESA DataStore.
event forwarding	The process by which an administrator forwards events to another SESA Manager. Event forwarding includes the ability to filter events selectively before forwarding.

event logging	The process by which SESA Agents collect product events and deliver them to the SESA Manager for insertion into the SESA DataStore.
exposed host	A method of making all ports on a LAN-side host available to the external (WAN-side) network. So, for example, if you are running multiple services (Telnet, Web, FTP, and so on) on an exposed host, these are accessible from the external WAN network using the WAN IP address. Pre-defined security gateway rules override this feature and forward packets for the defined service to the pre-defined LAN host.
file transfer	The process of using communications to send a file from one computer to another. In communications, a protocol must be agreed upon by sending and receiving computers before a file transfer can occur. See also TFTP.
filter	A program or section of code that is designed to examine each input or output request for certain qualifying criteria and then process or forward it accordingly. See also content filtering.
firewall	A program that protects the resources of one network from users on other networks. Typically, an enterprise with an intranet that lets its workers access the wider Internet uses a firewall to prevent outsiders from accessing its own private data resources.
firewall denial of service	A denial of service attack aimed directly at the firewall.
firmware	Operational code that contains all the features and functions of a hardware appliance. Firmware can usually be upgraded to add fixes or enhancements.
flash	Physical hardware component that stores data, usually firmware and configuration settings, on a hardware appliance. Flash data is not lost when the appliance is powered off.
flooding program	A program that contains code that, when executed, bombards the selected system with requests in an effort to slow down or shut down the system.
FQDN (fully qualified domain name)	A URL that consists of a host and domain name, including a top-level domain. For example, www.symantec.com is a fully qualified domain name. www is the host, symantec is the second-level domain, and .com is the top-level domain. An FQDN always starts with a host name and continues to the top-level domain name, so www.sesa.symantec.com is also an FQDN.
FTP (File Transfer Protocol)	A method to exchange files between computers. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers email, FTP is an application protocol that uses the Internet's TCP/IP protocols. See also TFTP.
gateway	A network point that acts as an entrance to another network. In a company network, a proxy server acts as a gateway between the internal network and the Internet. A gateway is also any computer or service that passes packets from one network to another network. See also default gateway, security gateway.
global tunnel	A VPN tunnel definition that applies to all outbound traffic from the host or gateway. For example, a global VPN tunnel is defined at a branch office gateway to the main office. The branch office will forward all traffic destined for the Internet into the VPN tunnel so that the main office firewalls can filter it before going to the Internet.
HTML (Hypertext Markup Language)	A standard set of commands used to structure documents and format text so that it can be used on the Web.
HTTP (Hypertext Transfer Protocol)	The set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Part of the TCP/IP suite of protocols (the basis for information exchange on the Internet), HTTP is an application protocol.
HTTPS (Hypertext Transfer Protocol Secure)	A variation of HTTP that is enhanced by a security mechanism, which is usually Secure Sockets Layer (SSL).
IKE (Internet Key Exchange)	A key management protocol standard that is used in conjunction with the IPSec standard. IPSec is an IP security feature that provides robust authentication and encryption of IP packets. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside of the Internet Security Association and Key Management Protocol (ISAKMP) framework. ISAKMP, Oakley, and Skeme are security protocols implemented by IKE. See also IPSec.

inbound rule A defined security gateway rule that allows or denies inbound traffic (all inbound traffic is blocked by default). Inbound rules are configured to match specific protocols or services (like FTP or Web) and you can apply them to different computer groups. For example, use an inbound that grants access to the universe (all computers) for HTTP when hosting a publicly-accessible Web server behind the behind the security gateway.

initialize To prepare for use. In communications, to set a modem and software parameters at the start of a session.

integrating product A security product that uses a SESA Agent to enable centralized event logging, alert management, and configurations distribution.

Internet Different, intercommunicating networks funded by both commercial and government organizations. It connects networks in many countries. No one owns or runs the Internet. There are thousands of enterprise networks connected to the Internet, and there are millions of users, with thousands more joining every day.

intranet An in-house Web site that serves the employees of the enterprise. Although intranet pages may link to the Internet, an intranet is not a site accessed by the general public.

intrusion detection A security service that monitors and analyzes system events for the purpose of finding and providing real-time, or near real-time, warning of attempts to access system resources in an unauthorized manner.

intrusion protection A system of automatically acting upon intrusion detection information to block (also called gating) the intrusion attempt's network traffic without user intervention.

IP (Internet Protocol) The method or protocol by which data is communicated from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one address that uniquely identifies it to all other computers on the Internet.

IP address A unique number that identifies a workstation on a network and specifies routing information. Each workstation on a network must be assigned a unique IP address, which consists of the network ID, plus a unique host ID assigned by the network administrator. This address is usually represented in dotted-quad notation, with the decimal values separated by a period (for example 192.168.0.1).

IP spoofing An attack method by which IP packets are sent with a false source address, which may try to circumvent security gateways by adopting the IP address of a trusted source. This fools the security gateway into thinking that the packets from the attacker are actually from a trusted source. IP spoofing can also be used simply to hide the true origin of an attack.

IPSec (Internet Protocol Security) A standard for security at the network or packet-processing layer of network communication. IPSec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both the authentication of the sender and encryption of data as well. IPSec is widely used with virtual private networks. See also IKE.

ISDN (Integrated Services Digital Network) A high-speed, digital, high-bandwidth telephone line that allows simultaneous voice and data transmission over the same line. ISDN is one of the always-on or dedicated class of connections.

ISP (Internet service provider) An organization or company that provides dial-up or other access to the Internet, usually for money.

key A variable value in cryptography that is applied (using an algorithm) to a string or block of unencrypted text to produce encrypted text. A key is also a series of numbers or symbols that are used to encode or decode encrypted data. See also shared key, private key.

LAN (local area network) A group of computers and other devices in a relatively limited area, such as a single building, that are connected by a communications link that enables any device to interact with any other device on the network.

leased line A telephone channel that is leased from a common carrier for private use. A leased line is faster and quieter than a switched line, but generally more expensive.

local attack An attack against a computer or a network to which the attacker already has either physical or legitimate remote access. This can include the computer that the attacker is using or a network to which that computer is connected.

log 1. A record of actions and events that take place on a computer. 2. The act of creating messages based on events and storing them in a file.

logging The process of storing information about events that occurred on the security gateway or network.

logon procedure	The process of identifying oneself to a computer after connecting to it by means of a directly connected keyboard or over a communications line. During the logon procedure, the computer usually requests a user name and password. On a computer used by more than one person, the logon procedure identifies authorized users, keeps track of their usage time, and maintains security by controlling access to sensitive files or actions.
MAC (Media Access Control)	On a network, a computer's unique hardware number. The MAC address is used by the Media Access Control sublayer of the Data Link Control (DLC) layer of telecommunication protocols. There is a different MAC sublayer for each physical device type. The data-link layer is the protocol layer in a program that handles the moving of data in and out across a physical link in a network.
main mode	An ISAKMP (IKE) negotiation typically used for gateway-to-gateway VPN tunnels where the originating IP address of both parties is known. More secure than the abbreviated aggressive mode, which doesn't use IP source as part of the authentication exchange. See also aggressive mode.
MIME (Multipurpose Internet Mail Extensions)	A protocol for transmitting documents with different formats over the Internet.
modem	A device that enables a computer to transmit information over a standard telephone line. Modems can transmit at different speeds or data transfer rates. See also bps.
monitoring	The viewing of activity in a security environment, generally in real-time. Monitoring lets administrators view the content of applications that are being used.
multicast	A bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to the members of a multicast group. Using a multicast router, packets sent from a single source are reviewed, replicated, and sent to all members in the multicast group.
multicasting	A method of cloning packets and sending them to a group of computers simultaneously across a network.
name server	A computer running a program that converts domain names into appropriate IP addresses and vice versa. See also DNS.
NAT (Network Address Translation)	A technique that hides a packet's real source or destination address by changing it to different IP address. For example, a security gateway might change the source IP address of a packet that originates from a protected host to the same IP address as the security gateway's outside interface. This results in all external hosts thinking that the packet originated from the security gateway, thus effectively hiding the real source host.
NAT (Network Address Translation) pool	A set of addresses that are designated as replacement addresses for client IP addresses. You can use this NAT pool addressing capability to conserve IP addresses, resolve address conflicts, and create virtual clients.
network	A group of computers and associated devices that are connected by communications facilities (both hardware and software) for the purpose of sharing information and peripheral devices such as printers and modems. See also LAN (local area network).
NIDS (network-based intrusion detection system)	A type of intrusion detection system that works at the network level by monitoring packets on the network and gauging whether a hacker is attempting to sending a large number of connection requests to a computer on the network, indicating an attempt either to break into a system or cause a denial of service attack. Unlike other intrusion detection systems, a NIDS is able to monitor numerous computers at once.
NNTP (Network News Transfer Protocol)	The predominant protocol used by computers (servers and clients) for managing the notes posted on newsgroups. NNTP replaced the original Usenet protocol, UNIX-to-UNIX.
node	In a network, an addressable device that is attached to the network and can recognize, process, or forward data transmissions.
NTP	A protocol used to synchronize or set the real-time clock in a computer or appliance. There are numerous publicly available primary and secondary servers in the Internet that are synchronized to the Coordinated Universal Time (UTC).
null modem cable	A cable that enables two computers to communicate without the use of modems. A null modem cable accomplishes this by crossing the sending and receiving wires so that the wire used for transmitting by one device is used for receiving by the other and vice versa.
online	The state of being connected to the Internet. When a user is connected to the Internet, the user is said to be online.

OS (operating system) The interface between the hardware of the computer and applications (for example a word-processing program). For personal computers, the most popular operating systems are MacOS, Windows, DOS, and Linux.

outbound rule A defined security gateway rule that allows or denies outbound traffic. Outbound rules are configured to match specific protocols or services (like FTP or Web) and you can apply them to different computer groups on the LAN. For example, you may have a computer group defined that has three outbound rules to allow email, Web, and DNS traffic only.

packet A unit of data that is formed when a protocol breaks down messages that are sent along the Internet or other networks. Messages are broken down into standard-sized packets to avoid overloading lines of transmission with large chunks of data. Each of these packets is separately numbered and includes the Internet address of the destination. Upon arrival at the recipient computer, the protocol recombines the packets into the original message.

packet sniffing The interception of packets of information (for example, a credit card number) that are traveling across a network.

password A unique string of characters that a user types as an identification code to restrict access to computers and sensitive files. The system compares the code against a stored list of authorized passwords and users. If the code is legitimate, the system allows access at the security level approved for the owner of the password.

perfect forward secrecy A method in VPN of creating new short-term cryptography keys that cannot be inferred from a compromised long-term (usually the original pre-shared key) or previous session key. Diffie-Hellman is the algorithm used for current PFS implementations.

physical address See MAC address.

ping (Packet INternet Groper) A program that system administrators and attackers use to determine whether a specific computer is currently online and accessible. Pinging works by sending an ICMP packet to the specified IP address and waiting for an ICMP reply; if a reply is received, the computer is deemed to be online and accessible.

PKI (public key infrastructure) An infrastructure that enables users of a basically nonsecure public network (such as the Internet) to exchange data securely and privately through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

policy See VPN policy.

port 1. A hardware location used for passing data into and out of a computing device. Personal computers have various types of ports, including internal ports for connecting disk drives, monitors, and keyboards, and external ports, for connecting modems, printers, mouse devices, and other peripheral devices. 2. In TCP/IP networks, the name given to an endpoint of a logical connection. Port numbers identify types of ports. For example, both TCP and UDP use port 80 for transporting HTTP data.

port scan An intrusion method in which attackers use software tools called port scanners to find services currently running on target systems. This is done by scanning the target for open ports, usually by sending a connection request to each port and waiting for a response. If a response is received, the port is known to be open.

PPP (Point-to-Point Protocol) A protocol used for communication between two computers. This is most commonly seen with dial-up accounts to an ISP. However, Point-to-Point Protocol over Ethernet (PPPoE) has now become more popular with many DSL providers.

PPPoE (Point-to-Point Protocol over Ethernet) A standard for incorporating the popular PPP protocol, widely used for dial-up Internet connections, into a dedicated modem connection that uses Ethernet as its transport at the carrier's facilities. Used by a large number of DSL modem providers, PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point connection to be established in the normally multipoint architecture of Ethernet.

PPTP (Point-to-Point Tunneling Protocol) A protocol from Microsoft that is used to create a virtual private network (VPN) over the Internet. Remote users can access their corporate networks using any gateway that supports PPTP on its servers. Some ISPs use PPTP as an authentication method (similar to PPP or PPPoE). PPTP is based on the point-to-point protocol (PPP) protocol and the generic routing encapsulation (GRE) protocol.

prefix A code that is required before a telephone number (it can be any number of digits). For example, the number 9 is often required to call out from many office Private Branch eXchange (PBX) systems.

preshared key Also called shared secret. The original key used to encrypt the initial two-way authentication exchange before creation encryption and authentication keys in an IKE-based VPN tunnel (also used in other authentication exchanges). Pre-shared keys must be known in advance by both parties to complete authentication.

primary server	A computer that is running Symantec AntiVirus Corporate Edition Server software that is responsible for configuration and virus definitions files update functions in a server group. When you perform a task at the server group level in Symantec System Center, the task runs on the primary server. The primary server forwards the task to its secondary servers. If the primary server is running Alert Management System2, it processes all alerts.
private key	A part of asymmetric encryption that uses a private key in conjunction with a public key. The private key is kept secret, while the public key is sent to those with whom a user expects to communicate. The private key is then used to encrypt the data, and the corresponding public key is used to decrypt it. The risk in this system is that if either party loses the key or the key is stolen, the system is broken.
protocol	A set of rules for encoding and decoding data so that messages can be exchanged between computers and so that each computer can fully understand the meaning of the messages. On the Internet, the exchange of information between different computers is made possible by the suite of protocols known as TCP/IP. Protocols can be stacked, meaning that one transmission can use two or more protocols. For example, an FTP session uses the FTP protocol to transfer files, the TCP protocol to manage connections, and the IP protocol to deliver data.
proxy	An application (or agent) that runs on the security gateway and acts as both a server and client, accepting connections from a client and making requests on behalf of the client to the destination server. There are many types of proxies, each used for specific purposes. See also gateway, proxy server.
proxy server	A server that acts on behalf of one or more other servers, usually for screening, firewall, caching, or a combination of these purposes. A proxy server, sometimes called a gateway, is typically used within a company or enterprise to gather all Internet requests, forward them out to Internet servers, and then receive the responses and in turn forward them to the original requester within the company.
public key	A part of asymmetric encryption that operates in conjunction with the private key. The sender looks up the public key of the intended recipient and uses the public key to encrypt the message. The recipient then uses his or her private key, which is known only to the recipient, to decrypt the message.
RADIUS	Remote Authentication Dial-In User Service: An access control protocol that uses a challenge/response method for authentication. Used to authenticate users for access to network resources.
RAM (Random Access Memory)	The memory that information required by currently running programs is kept in, including the program itself. Random access refers to the fact that any program can read from or write to any memory register. Many operating systems limit access to defined memory addresses to protect critical, occupied, or reserved RAM locations from tampering.
remote access	The use of programs that allow access over the Internet from another computer to gain information or to attack or alter your computer.
remote communication	The interaction with a host by a remote computer through a telephone connection or another communications line, such as a network or a direct serial cable connection.
remote management	A method of managing the configuration of a product from remote sites other than through a dedicated local management station. Usually performed with the same interface or look-and-feel as a local management session.
reset	An action that clears any changes made since the last apply or reset action.
response	The resulting action taken for a predefined event or incident based on predefined criteria.
revision	A collection of configuration settings at any moment in time. As the user makes changes to and validates a configuration, revisions are created within the SESA framework. These revisions are not made visible to the user.
RIP (Routing Information Protocol)	The oldest dynamic routing protocol on the Internet and the most commonly used dynamic routing protocol on local area IP networks. Routers use RIP to periodically broadcast routing information for the networks that they know how to reach.
roaming	A wireless network made up of multiple access points that allows seamless movement from one coverage area to another without leaving the network or interruption of service. See also cell.
ROM (read-only memory)	The memory that is stored on the hard drive of the appliance. Its contents cannot be accessed or modified by the computer user, but can only be read.
router	A device that helps local area networks (LANs) and wide area networks (WANs) achieve interoperability and connectivity.

rule	A logical statement that lets you respond to an event based on predetermined criteria.
run	To execute a program or script.
secondary server	A computer that is running Symantec AntiVirus Corporate Edition Server software that is a child of a primary server. In a server group, all secondary servers retrieve information from the same primary server. If the secondary server is a parent server, it in turn passes information on to its managed clients.
secure browser	A Web browser that can use a secure protocol, such as SSL, to establish a secure connection to a Web server. Netscape Navigator and Internet Explorer both offer this feature.
security	The policies, practices, and procedures that are applied to information systems to ensure that the data and information that is held within or communicated along those systems is not vulnerable to inappropriate or unauthorized use, access, or modification and that the networks that are used to store, process, or transmit information are kept operational and secure against unauthorized access. As the Internet becomes a more fundamental part of doing business, computer and information security are assuming more importance in corporate planning and policy.
security architecture	A plan and set of principles that describe the security services that a system is required to provide to meet the needs of its users, the system elements required to implement the services, and the performance levels required in the elements to deal with the threat environment.
security domain	A grouping of systems for security purposes. A security domain can be based on many system attributes, such as operating system, location, function, and role.
security gateway	A network entity that defines the gateway that serves as the point of decryption and encryption for the network.
security lifecycle	The cycle of threat awareness, policy definition, policy implementation, and policy monitoring.
security policy	1. A company's formal declaration of its security goals and how it will meet those goals. At its most fundamental level, a security policy is an organization of controls that is designed to reduce risk, demonstrate fiduciary responsibility, and satisfy regulatory code. 2. A set of security modules, such as the rules for constructing passwords or the ownership of a system's start-up procedures. Policies establish which users can access certain information, and point to the standards and guidelines that describe the necessary security checks.
security response	The process of research, creation, delivery, and notification of responses to viral and malicious code threats and operating system, application, and network infrastructure vulnerabilities. See also notification.
security risk	A known program that may or may not be a threat to a computer. For example, an email greeting that acts like a mass mailer, but isn't strictly a worm because you can choose to use it before it activates.
serial communication	The transmission of information between computers or between computers and peripheral devices one bit at a time over a single line (or a data path that is 1 bit wide). Serial communications can be either synchronous or asynchronous. The sender and receiver must use the same data transfer rate, parity, and flow control information. Most modems automatically synchronize to the highest data transfer rate that both modems can support. pcAnywhere uses the asynchronous communications standard for personal computer serial communications.
serial interface	A data transmission scheme in which data and control bits are sent in a 1-bit wide data path sequentially over a single transmission line. See also RS-232-C standard.
serial port	A location for sending and receiving serial data transmissions. Also known as a communications port or COM port. DOS references these ports by the names COM1, COM2, COM3, and COM4.
serial transmission	The transmission of discrete signals one after the other. In communications and data transfer, serial transmission involves sending information over a single wire one bit at a time. This is the method used in modem-to-modem communications over telephone lines.
server	Hardware or software that provides services to other computers (known as clients) that request specific services. Common examples are Web servers and mail servers.
service level agreement	An agreement between the party providing incident response and the party being protected. Service level agreements include time allotments for the contain, eradicate, recover, and follow-up phases of incident response.
services	Refers to different types of network resources like Web, FTP and SMTP. Services are defined by their port number and protocol type (TCP, UDP, ICMP). For example, the Web (HTTP) service uses the TCP protocol over port 80.

SESA (Symantec Enterprise Security Architecture)	The centralized, scalable management architecture that is used by Symantec's security products.
SESA Foundation Pack	The installation software for SESA.
SESA Integration Wizard	A Java application that is used to install the SESA Integration Package (SIP). See also SIPI (Symantec Integrated Product Installer).
SESA native product	A Symantec product that is built on the SESA foundation and therefore can leverage additional capabilities in SESA.
SESA non-native security product	See integrating product.
SESA-enabled product	A security application that is designed to forward events for inclusion in the SESA DataStore. See also SESA-integrated product.
SESA-integrated product	Any of the Symantec or non-Symantec security products from which SESA can receive events or to which SESA can relay events. Some products can be natively integrated through SESA, which provides additional capabilities and functions. See also SESA native product.
session	In communications, the time during which two computers maintain a connection and, usually, are engaged in transferring information.
SGMI (Security Gateway Management Interface)	The local management interface that is used to configure and manage an individual Symantec security gateway.
signature	1. A state or pattern of activity that indicates a violation of policy, a vulnerable state, or an activity that may relate to an intrusion. 2. Logic in a product that detects a violation of policy, a vulnerable state, or an activity that may relate to an intrusion. This can also be referred to as a signature definition, an expression, a rule, a trigger, or signature logic. 3. Information about a signature including attributes and descriptive text. This is more precisely referred to as signature data.
SIP (SESA Integration Package)	The data that SESA requires for each SESA-integrated product. This data lets SESA recognize the integrating product.
SIPI (Symantec Integrated Product Installer)	The registration software for the SESA Integration Package (SIP).
slider	A control for setting a value on a continuous range of possible values, such as screen brightness, mouse-click speed, or volume.
smart card	A plastic card about the size of a credit card that has an embedded microchip that can be loaded with data, used for telephone calling, electronic cash payments, and other applications, and then periodically recharged for additional use. Smart cards are currently used to establish identity when logging on to an Internet access provider.
SMTP (Simple Mail Transfer Protocol)	The protocol that allows email messages to be exchanged between mail servers. Then, clients retrieve email, typically via the POP or IMAP protocol.
SNMP (Simple Network Management Protocol)	The protocol governing network management and the monitoring of network devices and their functions.
software	The instructions for the computer to perform a particular task. A series of instructions that performs a particular task is called a program. Software instructs the hardware of the computer how to handle data to perform a specific task.
SPI (Security Parameter Index)	An Authentication Header (AH) SPI number between 1 and 65535 that you assign to each tunnel endpoint when using AH in a VPN policy.
spoofing	The act of establishing a connection with a forged sender address. This normally involves exploiting a trust relationship that exists between source and destination addresses or systems.
SSL (Secure Sockets Layer)	A protocol that allows mutual authentication between a client and server and the establishment of an authenticated and encrypted connection, thus ensuring the secure transmission of information over the Internet.
static tunnel	A VPN tunnel that has manually entered authentication and encryption keys. These keys do not change or get re-keyed automatically as in an IKE-based VPN tunnel.

subnet address A portion of an IP address that is used to poll all 254 nodes on a designated network for pcAnywhere hosts. For example, an entry of 127.2.3.255 displays all pcAnywhere hosts with IP addresses beginning with 127.2.3.

subnet entity A subnet address including the subnet mask.

suffix A code appended to the end of a telephone number for billing purposes, for example, a calling card number.

switched line A standard dial-up telephone connection; the type of line that is established when a call is routed through a switching station. See also leased line.

Symantec management console A Web-based console that provides SESA content viewing and management capabilities, letting administrators perform event management, group management, and security policy configuration management.

SYN attack A type of attack. When a session is initiated between the Transmission Control Program (TCP) client and server in a network, a very small buffer space exists to handle the handshaking (often referred to as the three-way handshake) or exchange of messages that sets up the session. The session establishing includes a SYN field that identifies the sequence in the message exchange. An attacker can send a number of connection requests very rapidly and then fail to respond to the reply. This leaves the first packet in the buffer so that other, legitimate connection requests can't be accommodated. Although the packet in the buffer is dropped after a certain period of time without a reply, the effect of many of these bogus connection requests is to make it difficult for legitimate requests for a session to get established. In general, this problem depends on the operating system providing correct settings or allowing the network administrator to tune the size of the buffer and the time-out period.

synchronous transmission A form of data transmission in which information is sent in blocks of bits separated by equal time intervals. The sending and receiving devices must first be set to interact with one another at precise intervals, then data is sent in a steady stream. See also asynchronous transmission.

SYSLOG (SYStem LOG protocol) A transport mechanism for sending event messages across an IP network. The receiving server is known as an "event message collector" or Syslog server.

system A set of related elements that work together to accomplish a task or provide a service. For example, a computer system includes both hardware and software.

task A series of steps to be performed on all selected computers. For example, creating an image file, cloning an image file, and applying configuration settings are all tasks.

TCP (Transmission Control Protocol) The protocol in the suite of protocols known as TCP/IP that is responsible for breaking down messages into packets for transmission over a TCP/IP network such as the Internet. Upon arrival at the recipient computer, TCP is responsible for recombining the packets in the same order in which they were originally sent and for ensuring that no data from the message has been misplaced in the process of transmission.

TCP/IP (Transmission Control Protocol/Internet Protocol) The suite of protocols that lets different computer platforms using different operating systems (such as Windows, MacOS, or UNIX) or different software applications communicate. Although TCP and IP are two distinct protocols, each of which serves a specific communicational purpose, the term TCP/IP is used to refer to a set of protocols, including Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and many others. This set of protocols lets computers on the Internet exchange different types of information using different applications.

Telnet The main Internet protocol for creating an interactive control connection with a remote computer. Telnet is the most common way of establishing a remote connection to a network, as with telecommuters or remote workers.

TFTP Trivial File Transfer Protocol: A version of the FTP protocol that has no directory or password capability. Used for file transfers with low network or application overhead, like sending firmware to an appliance for flashing.

threshold The number of events that satisfy certain criteria. Administrators define threshold rules to determine when notifications are to be delivered.

time-out A predetermined period of time during which a given task must be completed. If the time-out value is reached before or during the execution of a task, the task is canceled. You can configure a pcAnywhere host to disconnect from a remote computer after a certain amount of time has passed without activity.

Trojan horse A rogue program that disguises itself as a legitimate file to lure users to download and run it. It takes the identity of a trusted application to collect confidential user information or avoid detection. A Trojan horse neither replicates nor copies itself, but causes damage and compromises the security of an infected computer.

tunnel	A process that lets a company securely use public networks as an alternative to using its own lines for wide-area communications. See also dynamic tunnel, static tunnel, global tunnel.
UDP (User Datagram Protocol)	A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. UDP is used primarily for broadcasting messages over a network.
universe entity	A permanent security gateway host entity. The universe entity is similar to a wildcard and specifies the set of all computers. The universe entity's associated IP address is 0.0.0.0.
upload	To send a file from one computer to another via modem, network, or serial cable. With a modem-based communications link, the process generally involves the requesting computer instructing the remote computer to prepare to receive the file on its disk and wait for the transmission to begin. See also download.
UPS (uninterruptible power supply)	A device that lets your computer and firewall equipment run for a short time after a power failure, which lets you power the computer or firewall equipment down in an orderly manner. A UPS also provides protection in the event of a power surge.
URL (Uniform Resource Locator)	The standard addressing system for the World Wide Web. A URL consists of two parts: The first part indicates the protocol to use (for example http://), and the second part specifies the IP address or the domain name and the path where the desired information is located (for example www.securityfocus.com/glossary).
URL blocking	The tracking and denying of user access to undesirable Web sites based on predefined site content. See also content filtering.
user authentication	A process that verifies a user's identity to ensure that the person requesting access to the private network is, in fact, that person to whom entry is authorized.
user name	A form of authentication that is in place to ensure that the user is authorized to use the services being requested. The user name also signifies the primary user or users of a particular computer.
virus	A piece of programming code inserted into other programming to cause some unexpected and, for the victim, usually undesirable event. Viruses are transmitted by programs downloaded from other sites or present on a diskette. The source of the file you are downloading or retrieving from a diskette is often unaware of the virus. The virus lies dormant until circumstances cause the computer to execute its code. Some viruses are playful in intent and effect, but some can be harmful, erasing data or causing your hard disk to require reformatting.
virus definitions file	A file that provides information to antivirus software for finding and repairing viruses. In Symantec AntiVirus Corporate Edition, the administrator must regularly distribute updated virus definitions files to Symantec AntiVirus Corporate Edition servers and clients.
virus scanner	A program that searches files (including email and attachments) for possible viruses.
VPN (virtual private network)	A network that has characteristics of a private network such as a LAN, but which is built on a public network such as the Internet. VPNs let organizations implement private networks between geographically separate offices and remote or mobile employees by means of encryption and tunneling protocols.
VPN group	A defined group of users with certain VPN network configurations and policy settings associated with them. For example, Group 2 VPN users may have antivirus policy enforcement enabled for them.
VPN policy	The parameters that define a VPN tunnel are keying, encryption and authentication methods, and strengths.
WAN (wide area network)	A network that connects distant sites through links provided by local telephone companies. Typically, a WAN extends a local area network (LAN) outside of a building to link to other LANs in remote buildings, possibly in remote cities.
Web attack	An attack from the outside that is aimed at Web server vulnerabilities.
Web browser	A client program that uses the Hypertext Transfer Protocol (HTTP) to make requests of Web servers throughout the Internet on behalf of the browser user.
Web denial of service	A denial of service attack that specifically targets a Web server.

wildcard character A symbol that enables multiple matching values to be returned based on a shared feature. The script language has two wildcards: the question mark (?) and the asterisk (*). The question mark stands for any single character, and the asterisk stands for any character string of any length. For example, the file specification *.* would return all files, regardless of their file names; the file specification *.sc? would return all file names that have a three-character extension beginning with sc (such as compusrv.scr, compusrv.scx, and so on).

wizard A tool that makes configuration tasks faster and easier. The wizard prompts the user by requesting data and walking the user through the specific set procedure. From the first Wizard screen, users have the option of closing the Wizard and working from the appropriate Property Pages.

workstation 1. A networked computer that is using server resources. 2. A computer that is connected to a mainframe computer. It is usually a personal computer connected to a local area network (LAN) that shares the resources of one or more large computers. Workstations differ from terminals or dumb terminals in that they can be used independently from the mainframe. They can have their own applications installed and their own hard disks. 3. A type of computer that requires a significant amount of computing power and is capable of producing high-quality graphics.

worm A special type of virus. A worm does not attach itself to other programs like a traditional virus, but creates copies of itself, which create even more copies.

WWW (World Wide Web) An application on the Internet that allows for the exchange of documents formatted in Hypertext Markup Language (HTML), which facilitates text, graphics, and layout. As the World Wide Web has grown in popularity, its capabilities have expanded to include the exchange of video, audio, animation, and other specialized documents. The World Wide Web is also a system of Internet servers that support specially formatted documents. Another important aspect of the World Wide Web is the inclusion of hypertext links that allow users to click links and quickly navigate to other related sites.

Index

Numerics

3DES 74

A

administration password 18
Administration settings 17
    Advanced Management 122
    Basic Management 18, 20, 121
    LiveUpdate 98, 101, 124
    SNMP 95, 123
    Trusted Certificates 123
administrative access 18
Advanced connection settings 38
Advanced Firewall tab 62, 63, 143
Advanced IDS and IPS tab 91, 155
Advanced Management tab 122
advanced options 62
advanced protection settings 91
Advanced VPN tab 69, 79, 153
Advanced WAN/ISP tab 39, 44, 136
AES-128 74
AES-192 74
AES-256 74
alive indicator 28, 36, 45
all.bin 100
allow list 86
analog connections 29
antivirus clients 85
Antivirus Policy settings 17, 156
    AVpe 83
antivirus server status 85
app.bin firmware 97
appliance, front panel LEDs 105
Asymmetrical Digital Subscriber Line (ASDL) 30
atomic signature
    Bonk 89
    Fawx 89
    HTML buffer overflow 90
    Jolt 89
    Land 89
    Nestea 89
    Newtear 89
    Overdrop 89
    Ping of Death 89
    Syndrop 89
    TCP/UDP flood protection 90
    Teardrop 90
    Winnuke 90
attacks 89
automatic updates 98
AVpe 81
    configuring 82
    log messages 85
    overview 10
AVpe tab 83

B

backing up and restoring
    configurations 103
backing up and restoring configurations 160
backup dial-up account 35, 37
Basic Management tab 19, 20, 121
BattleNet 60
Bonk 89
broadband
    cable modem 29
broadband connection 29

C

cable modem 29
certificates 160
change
    administrator password 19
    appliance LAN IP address 49
    SGMI language 28
Channel Service Unit (CSU) 29
Client Tunnels tab 78, 84, 88, 149
Client Users tab 69, 150
client-to-gateway tunnels 76
client-to-gateway tunnels, global policy settings 79
clusters
    creating tunnels to Symantec Gateway 5400 Series clusters 72
command buttons 17
compression, tunnel 66
computer group membership 54
computer groups defining 55
Computer Groups tab 56, 84, 88, 138
computers and computer groups 53
Computers tab 54, 137
configuration, backing up and restoring 103
configuring
    advanced connection settings 38
    advanced options 62
    advanced PPP settings 39
    advanced protection settings 91
    advanced WAN/ISP settings 43
    appliance as DHCP server 50
    AVpe 82
    client-to-gateway tunnels 76
    computers 54
    connection to the outside network 23
    connectivity 30
    dial-up accounts 36
    dynamic gateway-to-gateway tunnels 72
    exposed host 64
    failover 45
    gateway-to-gateway tunnels 70

idle renew 38
internal connections 49
log preferences 93
Maximum Transmission Unit (MTU) 39
new computers 54
password 19
port assignments 51
PPTP 34
remote management 19
routing 42
special applications 60
static route entries 42
WAN port 28
configuring LAN IP settings 49
connecting manually, PPPoE 32
connecting to serial port 18, 21
connection to the outside network 23
connection types
analog 29
broadband 29
DHCP 29
ISDN 29
PPPoE 29
PPTP 29
static IP 29
understanding 29
connections
network examples 24
connectivity,configuring 30
content filtering 86
allow list 86
deny lists 86
LAN 87
managing lists 87
overview 10
WAN 79
Content Filtering settings 17, 87, 88, 157
creating
custom phase 2 VPN policies 67
security policies 66

D

default settings, restore port assignment 52
defining
computer group membership 54
inbound access 56
outbound access 57
deny list 86
DES 74
DHCP 29
connections 29
Force Renew 136
usage 51
DHCP server 50
DHCP settings
advanced settings 38
dial-up accounts 35
backup 37
back-up account 35
configuring 36
connecting manually 37
monitoring status 38
verifying connectivity 38
Dial-up Backup & Analog/ISDN tab 36, 130
Digital Service Unit (DSU) 29
disabling
dynamic DNS 41
NAT mode 62
disconnect idle PPPoE connections 30
DNS gateway 45
documentation 12
online help 16, 17
DSL 29
DSL connectivity 29
dual-WAN port 28
dynamic DNS
disabling 41
forcing updates 41
TZO 40
Dynamic DNS tab 40, 41, 133
dynamic gateway-to-gateway tunnels 72
dynamic routing 42
Dynamic Tunnels tab 73, 145

E

Email Log Now 93
emailing log messages 93
enabling
IDENT port 62
IPsec pass-thru 63
exposed host 64

F

failover 45
Fawx 89
Firewall settings 17
Advanced 62, 64, 143
Computer Groups 56, 84, 88, 138
Computers 54, 137
Inbound Rules 56, 139
Outbound Rules 58, 140
Services 60, 140
Special Applications 61, 141
firewall technology 10
firewall,Host List 55
firmware 97, 98, 100
app.bin 97
updates 97
upgrading manually 100
firmware upgrades 20
flash the firmware 101
flashing the appliance 18, 101
Force Renew 136
forcing dynamic DNS updates 41
front panel LEDs 105

G

games 60
gateway-to-gateway
supported VPN tunnels 71
gateway-to-gateway tunnels 70
dynamic tunnels 72
tunnel persistence and high-availability 71

Global IKE Policy 66
global policy settings, client-to-gateway tunnels 79

H

HA. *See* high availability
help 16
Help button 17
high availability 43
Host List 55
HTML buffer overflow 90

I

ICMP requests 36
IDENT port 62
idle renew 38
IDS and IPS
    overview 10
IDS and IPS settings 17
    Advanced 91, 155
    IDS Protection 90, 154
IDS Protection tab 90, 154
IKE tunnels, gateway-to-gateway tunnels 72
inbound rules 56
Inbound Rules tab 56
Inbound Ruls tab 139
internal connections 49
intrusion attempt
    Bonk 89
    Fawx 89
    HTML buffer overflow 90
    Jolt 89
    Land 89
    Nestea 89
    Newtear 89
    Overdrop 89
    Ping of Death 89
    Syndrop 89
    TCP/UDP flood protection 90
    Teardrop 90
    Trojan horse 90
    Winnuke 90
IP spoofing protection 91
IPsec pass-thru 63, 127, 143
ISDN connections 29

J

Join SESA 159, 162
    event management 163
    gathering connection information 161
    options 161
    preparation 160
    returning to local management 164
    tasks performed 159
    troubleshooting 164
Jolt 89

K

key features 9

L

LAN IP & DHCP tab 49, 50, 125
LAN IP address 49
LAN IP settings 49
LAN settings 17
    LAN IP & DHCP 49, 50, 125
    Port Assignments 51, 127
Land 89
LB. *See* load balancing
LEDs 105
Licensing 111
LiveUpdate 101
    overview 10
    server 98
    updates 98
LiveUpdate tab 98, 101, 124
load balancing 44
log messages 96
log messages,email forwarding 93
log preferences 93
Log Settings tab 94, 95
Logging/Monitoring settings 17
    Log Settings 94, 95
    Status 118
    Troubleshooting 121
    View Log 96, 119

M

MAC cloning 46
MAC masking 46
Main menu 16
Main Setup tab 30, 31, 34, 36, 128
managing
    administrative access 18
    content filtering lists 87
    using the serial console 21
manual dial-up accounts 37
manually
    connect to PPTP account 35
    upgrading firmware 100
manually reset password 19
Maximum Transmission Unit (MTU) 39
menu tabs 17
modem connectivity 36
monitoring
    antivirus server status 85
    DHCP usage 51
    dial-up accounts 38
monitoring VPN tunnel status 80

N

NAT mode 62
Nestea 89
network access,planning 53
network connections 29
network security best practices 13
network settings
    optional 46
network traffic control 53
network traffic control,advanced 81
Newtear 89

Norton Internet Security 100

O

online help 16
optional network settings 46
outbound rules 57
Outbound Rules tab 58, 140
outside network
    configuring connection 23
Overdrop 89

P

password
    administration 18
    configure 19
    manually reset 19
PING 36
Ping of Death 89
planning network access 53
Point-to-Point Protocol over Ethernet. *See* PPPoE
Point-to-Point-Tunneling Protocol (PPTP) 34
policy,Global IKE 66
Port assignments 51
Port Assignments tab 51, 127
PPP settings,advanced 39
PPPoE
    connecting manually 32
    connectivity 29
    defined 30
    Query Services 130
    verifying connectivity 32
PPPoE tab 32, 129
PPTP
    configuring for connectivity 34
    connecting manually 35
    manual connection 35
    TCP/IP based network 34
    verifying connectivity 34
PPTP connection 29
PPTP tab 34, 35, 132
preventing attacks 89
protection
    IP spoofing 91
    TCP flag validation 91
protection preferences
    configuring
        protection preferences settings 90
    settings 90

Q

Query Services 130
question mark 16

R

rear panel
    420 and 440 appliance 36
    460 and 460R 36
redirecting services 59
remote gateway administrator, sharing information 75
remote management 19
resetting the appliance 18, 104
restore port assignment default settings 52
restoring configurations 103, 160
routing 42
Routing tab 42, 134
routing,dynamic 42

S

scroll lock 21
secure VPN connections 65
Security Gateway Management Interface 10, 15
security policies 66
serial console 21
    HyperTerminal 21
    scroll lock 21
serial port 18
Services tab 60, 140
SESA
    joining 159
        event management 163
        gathering connection information 161
        importing configurations 162
        options 161
        preparation 160
        troubleshooting 164
    returning to local management 164
        temporarily 165
SESA Console
    logging on 164
Setup Wizard 18, 27
SGMI 10, 15
SMTP binding 44
SMTP time-outs 62
SNMP tab 95, 123
special applications 60
Special Applications tab 61, 141
static content filtering 10
static gateway-to-gateway tunnels 73
static IP 29
Static IP & DNS tab 33, 129
static route entries 42
Static Tunnels tab 75, 148
Status tab 118
subnet 71
Symantec Advanced Manager 11
Symantec Advanced Manager for Security Gateways
    joining SESA 162
        event management 163
    leaving SESA management 164
    returning to local management
        temporarily 165
Symantec Event Manager 11
Symantec Event Manager for Security Gateways
    joining SESA 163
    leaving SESA management 164
    returning to local management
        temporarily 165
Symantec Gateway Security 5400 Series 71, 72
Symantec management console 11
Syndrop 89
Syslog 94
System Setup Wizard 160

T

T1 29
TCP flag validation 91
TCP/IP-based network,PPTP 34
TCP/UDP flood protection 90
Teardrop 90
technical support 109
testing connectivity 45
TFTP 20, 100
time-outs, SMTP 62
traffic flow
  inbound access 56
  outbound access 57
Trojan horse protection 90
Troubleshooting 107
Troubleshooting tab 121
trusted certificates 160
Trusted Certificates tab 123
tunnel compression 66
tunnel configurations
  VPN
    gateway-to-gateway 70
tunnel negotiations
  Phase 1 67
  Phase 2 67
tunnels
  client-to-gateway 76
  dynamic gateway-to-gateway 72
TZO 40

U

understanding connection types 29
updating firmware 97
upgrading firmware
  Norton Internet Security 100

V

verifying PPPoE connectivity 32
video conferencing 60
View Log tab 96, 119
VPN
  authentication key lengths 74
  configuring client-to-gateway tunnels 76
  creating custom phase 2 policies 67
  creating tunnels to Symantec Gateway Security 5400 Series clusters 72
  encryption key lengths 74
  global policy settings 79
  monitoring tunnel status 80
  overview 10
  phase 2, configurable 67
  policies 66
  secure connections 65
  subnet 71
  supported gateway-to-gateway tunnels 71
  tunnel compression 66
  tunnel configurations 70
    client-to-gateway 76
    gateway-to-gateway 70
  tunnel high-availability 71
  tunnel negotiations
    Phase 1 66
    Phase 2 66
  tunnel persistence 71
  tunnel status 80
VPN Policies tab 67, 151
VPN settings 17
  Advanced 69, 79, 153
  Client Tunnels 78, 84, 88, 149
  Client Users 69, 150
  Dynamic Tunnels 73, 145
  Static Tunnels 75, 148
  VPN Policies 67, 151
  VPN Status 152
VPN Status tab 152
VPN tunnel
  remote management 19

W

WAN port
  configuration 23, 28
  configuring MTU 39
  connection 23
WAN/ISP
  advanced settings 43
  configuring idle renew 38
WAN/ISP multiple IP addresses 30
WAN/ISP settings 17
  Advanced 39, 43, 44, 46, 136
  Analog/ISDN 36
  DHCP 30
  Dial-up Backup & Analog/ISDN 37, 130
  Dynamic DNS 40, 41, 133
  Main Setup 45, 128
  PPPoE 31, 129
  PPTP 34, 132
  Routing 42, 134
  Static IP & DNS 33, 129
Winnuke 90
Wireless settings 17
wizards
  Join SESA 159
  System Setup 160